USER'S GUIDE

Release 1.2

Cabletron Systems

(603) 332-9400 phone
(603) 337-3075 fax
support@ctron.com

NOTICE

You may post this document on a network server for public use as long as no modifications are made to the document.

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

©Copyright 1998 by Cabletron Systems, Inc. All rights reserved.

Cabletron Systems, Inc.
P.O. Box 5005
Rochester, NH 03866-5005

Order Number: 9032431

VIRUS DISCLAIMER

Cabletron Systems has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Cabletron Systems makes no representations or warranties to the effect that the Licensed Software is virus-free.

Copyright © July 1997, by Cabletron Systems, Inc. All rights reserved.

TRADEMARKS

Cabletron Systems, CyberSWITCH, MMAC-Plus, SmartSWITCH, SPECTRUM, and SecureFast Virtual Remote Access Manager are trademarks of Cabletron Systems, Inc.

All other product names mentioned in this manual are trademarks or registered trademarks of their respective companies.

COPYRIGHTS

All of the code for this product is copyrighted by Cabletron Systems, Inc.

© Copyright 1991-1997 Cabletron Systems, Inc. All rights reserved. Printed in the United States of America.

Portions of the code for this product are copyrighted by the following corporations:

Epilogue Technology Corporation
Copyright 1991-1993 by Epilogue Technology Corporation. All rights reserved.

Livingston Enterprises, Inc.
Copyright 1992 Livingston Enterprises, Inc.

Security Dynamics Technologies Inc.
Copyright 1995 by Security Dynamics Technologies Inc. All rights reserved.

Stac Electronics
Stac Electronics 1993, including one or more U.S. Patents No. 4701745, 5016009, 5126739 and 5146221 and other pending patents.

Telenetworks
Copyright 1991, 92, 93 by Telenetworks. All rights reserved.

CABLETRON SYSTEMS, INC. PROGRAM LICENSE AGREEMENT

IMPORTANT: Before utilizing this product, carefully read this License Agreement.

This document is an agreement between you, the end user, and Cabletron Systems, Inc. ("Cabletron") that sets forth your rights and obligations with respect to the Cabletron software program (the "Program") contained in this package. The Program may be contained in firmware, chips or other media. BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

CONTENTS

Using this Guide 8
- About this Guide 8
- Documentation Set 9
- Guide Conventions 10

System Overview 11
- The SFVRA-CFG Network 12
- Interoperability Overview 16
  - Interoperability Protocols 16
  - Interoperability Devices 16
- System Components 17
- ISDN Network Devices 17
- System Requirements 18
  - SFVRA-CFG's Database PC Requirements 18
  - SFVRA-CFG's Application PC Requirements 18

System Installation 19
- Installing the SFVRA-CFG System 19
  - Installing When Using MS SQL Server 19
    - Installing the MS SQL Server 19
    - Installing the ODBC Drive Pack 3.0 19
    - Installing the SFVRA-CFG Software 21
    - Installing the SFVRA-CFG Database 22
      - Login Accounts 25
  - Installing When Using MS Access 26
    - Installing the ODBC Drive Pack 3.0 27
- Installing Adobe Acrobat Reader 27

Using the SFVRA-CFG Application 28
- Overview 28
- SFVRA-CFG Configuration Scenarios 28
  - New Network Configuration 29
  - Updates for an Established Network 30
  - Copying Updated Files 30
- Starting the SFVRA-CFG Application 31
- Configuration Building Blocks 31
- Using the SFVRA-CFG Menus 33
- System Messages 33

Configuring Tables 35
- Overview 35
- Configuring the Product Code Table 35
- Configuring the SFVRA Database Table 38

Configuring Site Templates 40
- Overview 40
- Adding a Site Template 41
- Configuring Template Physical Resources 43
  - Configuring Basic Rate (BRI) Resources 43
  - Configuring Primary Rate (PRI) Resources 44

Configuring V.35 or RS232 Resources 46
Configuring Digital Modem Resources 47
Configuring Template Options 47
Configuring MAC Layer Bridging Information 48
Configuring IP Information 49
Configuring IPX Information 51
Configuring AppleTalk Information 53
Configuring SNMP Information 54
Configuring PPP Information 55
Configuring Call Control Information 57
Configuring Default Line Protocol Information 59
Configuring Template Security Information 60
Configuring Template Connections Information 61
Configuring Authentication Information 61
Configuring Restriction Information 62
Configuring Access Information 64
Configuring Protocol Information 65
Configuring IP Information 65
Configuring IPX Information 66
Configuring AppleTalk Information 69
Configuring Bridging Information 70

Configuring Sites 71
Overview 71
Adding a Site 71
Configuring Site Properties 71
Configuring Contact Information 73
Configuring the Site's Systems 73

Configuring Circuits 79
Overview 79
Initial Steps 79
Configuring Circuit Properties 80
Configuring Circuit Data Links 81
Configuring Circuit Call Screening 83
Configuring Circuit Accesses 83

Configuring Connection Groups 85
Overview 85
Adding Connection Groups 85
Modifying Star Configurations 87
Modifying Connection Information 92
Adjusting Telephone Numbers 92
Entering Calling Line IDs 94
Adjusting Restriction Information 95
Adjusting Access Information 96
Adjusting Protocol Information 97

Configuring IP Network Information 99
Overview 99
IP Network Concepts 99
Network Interfaces 99
Static Routes 101
Configuring IP Network Subnet Information 102
Configuring IP Network Subnet Properties 103
Configuring IP Network Subnet Interfaces 105
Configuring IP Network Subnet Static Routes 109
Configuring IP Network Systems Information 112
Configuring IP Network System Properties 113
Configuring IP Network System Interfaces 114
Configuring IP Network System Static Routes 116
Configuring IP Filters 118

Configuring IPX Network Information 120
Overview 120
Configuring IPX Network Segment Information 120
Configuring IPX Network Segment Properties 121
Configuring IPX Network Segment Interfaces 122
Configuring IPX Network Systems Information 125
Configuring IPX Network System Properties 126
Configuring IPX Network System Interfaces 127

Configuring AppleTalk Network Information 129
Overview 129
Configuring AppleTalk Network Segment Information 129
Configuring AppleTalk Network Segment Properties 130
Configuring AppleTalk Network Segment Zones 131
Configuring AppleTalk Network Segment Ports 133
Configuring AppleTalk Network Segment Static Routes 134
Configuring AppleTalk Network System Information 137
Configuring AppleTalk Network System Properties 138
Configuring AppleTalk Network System Ports 139
Configuring AppleTalk Network System Static Routes 140

Configuring SNMP Management Groups 143
Overview 143
Configuring SNMP Management Group Properties 144
Configuring SNMP Management Group Communities 144
Designating SNMP Management Group Trap Receivers 145
Selecting SNMP Management Group Managed Sites 146

SFVRA-CFG Reports 147

Exporting Configuration Files 148
Overview 148
System Configuration Files 148
Generating Configuration Updates 149
Downloading Configuration Updates 150
Copying Configuration Updates 150

SFVRA Database Data 152
Generating SFVRA Database Data 153
Downloading SFVRA Database Data 153
Resetting SFVRA Database Data 155

Using SFVRA-CFG Options 156
Overview 156
Setting the Tool Bar Display 156
Confirming Database Actions 157
Setting Up and Using Search Filters 157
Setting the SFVRA-CFG Configuration Folder Path 159

Routine Maintenance 160
Overview 160
Configuration Back Up 160
Upgrading SFVRA-CFG Application Software 160
Upgrading SFVRA-CFG Database Software (Only if using MS SQL Server) 162

System Worksheets 164
Network Topology 165
System Details 166
Resources 166
Lines 166
Accesses 167
Device Information 168
Bridging and Routing Information 169
Bridging 169
IP Routing 169
IPX Routing 170
AppleTalk Routing 171

Getting Assistance 172
Reporting Problems 172
Contacting Cabletron Systems 172

INDEX 174

USING THIS GUIDE

This guide provides an overview as well as instructions for installing and configuring the SFVRA Configuration Manager (also referred to as SFVRA-CFG). This guide has been written for the network administrator responsible for setting-up, configuring, and maintaining networks configured using SFVRA-CFG.

ABOUT THIS GUIDE

The *User's Guide* is divided into the following chapters:

System Overview provides a basic description of the SFVRA-CFG network, an interoperability overview, a brief description of system components, and a list of system requirements.

System Installation provides a step-by-step description of installing your SFVRA-CFG.

Using the SFVRA-CFG Application provides instructions for starting up the SFVRA-CFG application, and also instructions for using the menu option and tool bars for configuration. A discussion of SFVRA-CFG system messages is also included.

Configuring Tables provides instructions for configuring a product code table and an SFVRA table. Information configured in these tables is incorporated later when entering other configuration information.

Configuring Site Templates provides instructions for defining SFVRA-CFG site templates. A site template is a time-saving tool, allowing you to configure a template of basic site information that can be used over and over when configuring similar sites.

Configuring Sites provides instructions for defining individual sites. For each site you will enter various site properties (including the site template you wish to use for this site), optional contact information, and the systems associated with this site.

Configuring Circuits provides instructions for defining the site's circuit information. Circuits are the physical WAN connections to each system. Circuit information includes line properties, and where applicable, data link and access information.

Configuring Connection Groups provides instructions for establishing connection groups among the configured sites. Connection groups allow you to divide a network into groups of sites that need to intercommunicate. Within each group, you can select a central site for the group, creating a star configuration.

Configuring IP Network Information provides instructions for defining IP subnets, then entering IP information for that subnet. This chapter also provides instructions for entering IP information for individual systems. IP network information defines how an IP network will interconnect.

Configuring IPX Network Information provides instructions for defining IPX segments, then entering IPX information for that segment. This chapter also provides instructions for entering IPX information for individual systems. IPX network information defines how an IPX network will interconnect.

Configuring AppleTalk Network Information provides instructions for defining AppleTalk segments, then entering AppleTalk information for that segment. This chapter also provides instructions for entering AppleTalk information for individual systems. AppleTalk network information defines how an AppleTalk network will interconnect.

Configuring SNMP Management Groups provides instructions for defining groups of sites that are collectively managed by an SNMP Manager.

SFVRA-CFG Reports provides instructions for generating reports that summarize the information you have configured using SFVRA-CFG.

Exporting Configuration Files provides instructions for incrementally updating a specific system's configuration, then transferring the new configuration files to the site.

Using SFVRA-CFG Options provides instructions for using the tool bar, confirming database actions, defining and using search filters, and setting the configuration folder path.

Routine Maintenance provides instructions for backing up the database files and for performing SFVRA-CFG application and database software upgrades.

APPENDICES

The *User's Guide* provides the following appendices:

NETWORK WORKSHEETS

These worksheets are provided to help you gather pertinent information for configuring your system. We recommend that you print copies of these blank forms and fill in the appropriate information before you begin configuring your system.

GETTING ASSISTANCE

This appendix provides information for getting assistance if you run into problems when installing your system. A FAX form is included. You can print this form, fill out the information requested, and FAX it to Cabletron Systems, using the provided FAX number.

DOCUMENTATION SET

This guide, the *User's Guide*, provides detailed information to install and configure your system. It also provides information you can use to keep your SFVRA-CFG running smoothly.

Context-sensitive help is available for fields within the user interface. To activate context-sensitive help, Windows NT users can use the mouse to select the field in question and press <F1>. Buttons can be selected by using the Tab key. Windows 95 users can use the right mouse button to click on the field in question.

The *Release Notes* provide release highlights and important information related to this release that you should review before you configure the SFVRA-CFG. The Release Notes are provided in a file that can be accessed under the SFVRA-CFG's Help menu.

GUIDE CONVENTIONS

The following conventions are used throughout the documentation:

SYSTEM COMMANDS

All commands are italicized, and in a different font than the general text. For example, if you are instructed to enter the path for the location of the NDIS driver, the command would appear as follows:

c:\Program Files\SFVRACFG\driver

DOCUMENTATION TITLES

All references to Documentation and Chapter titles will use the same font as normal text, but will be italicized. For example, all references to the chapter Configuring Functions will appear as:

Configuring Functions

SYSTEM OVERVIEW

The SFVRA-CFG allows a network consisting of Cabletron CyberSWITCH systems and/or SmartSwitch Remote Access Modules to be configured and managed centrally. It is made up of two main components: the SFVRA-CFG database (using either MS SQL Server, a Windows NT application, or MS Access, a Windows NT/Windows 95 application), and the SFVRA-CFG application, which runs on a Windows 95 or Windows NT device.

The SFVRA-CFG application is the interface to the database. Through the SFVRA-CFG application, the network administrator can generate each system's configuration files separately, with the system's view of the network, then download the configuration files electronically to the system. It is also important to note that downloading these configuration files does not update the system's existing configuration files, it overwrites them.

Once installed, the SFVRA-CFG application requires a connection to the SFVRA-CFG database. The application is connected by a 32-bit ODBC (Open Database Connectivity) software driver.

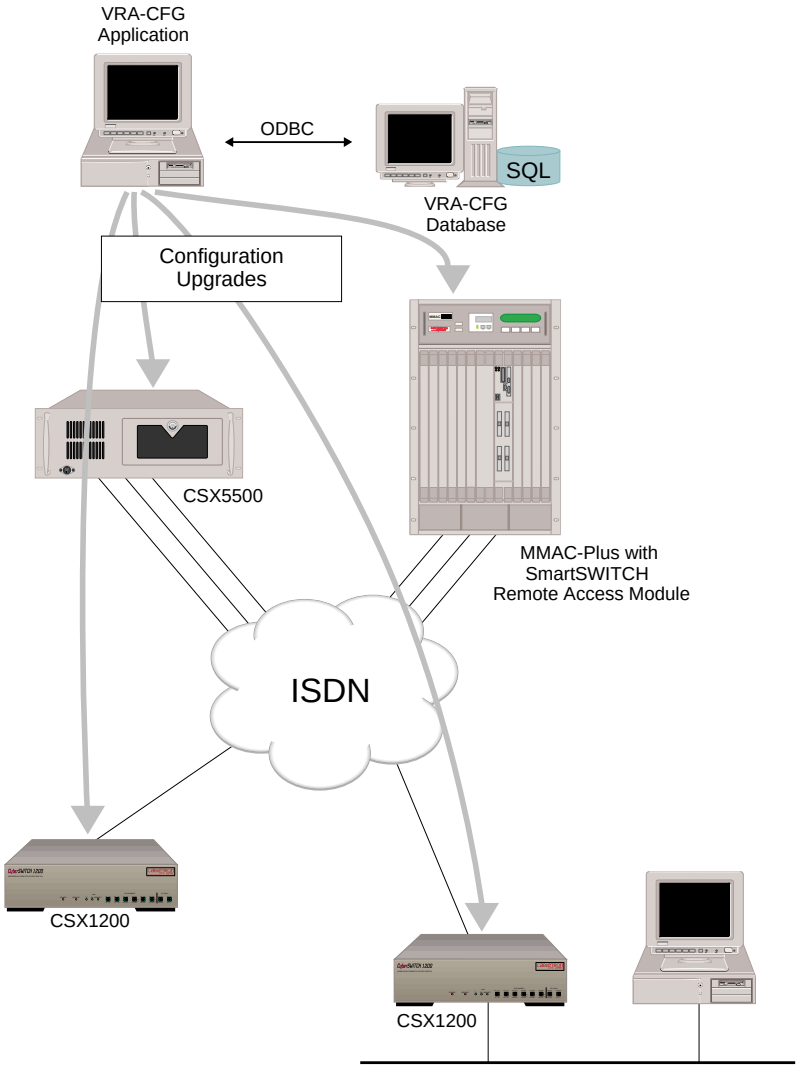
The SFVRA-CFG application can be run on multiple workstations simultaneously, with one central SFVRA-CFG database. This allows a large network to be managed by more than one network administrator.

For backup purposes, the administrator may archive versions of the database. The database can also be replicated onto multiple servers so that a hot-backup is always available.

For a network administrator, the SFVRA-CFG application provides the following features:

- Provides a quick mechanism to define a system at a site, based on administrator-defined templates and standard configurations.
- Allows the definition of the major protocol networks, mapping them to specific sites and then to systems at that site.
- Allows the definition of the network's ISDN circuits, and also the mapping of the circuits to sites and systems.
- Generates the configuration files for a specific system.
- Transfers the configuration files to a specific system using a proprietary, secure protocol.

The graphic below illustrates an SFVRA-CFG model using an MS SQL database.

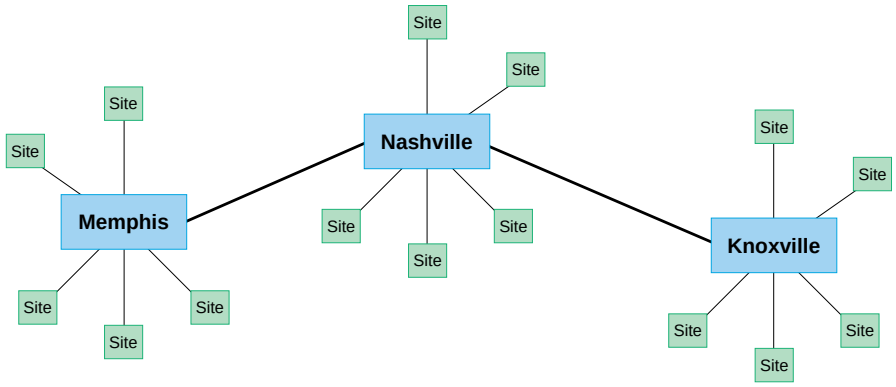


THE SFVRA-CFG NETWORK

The major concepts you need to understand to configure an SFVRA-CFG network are:

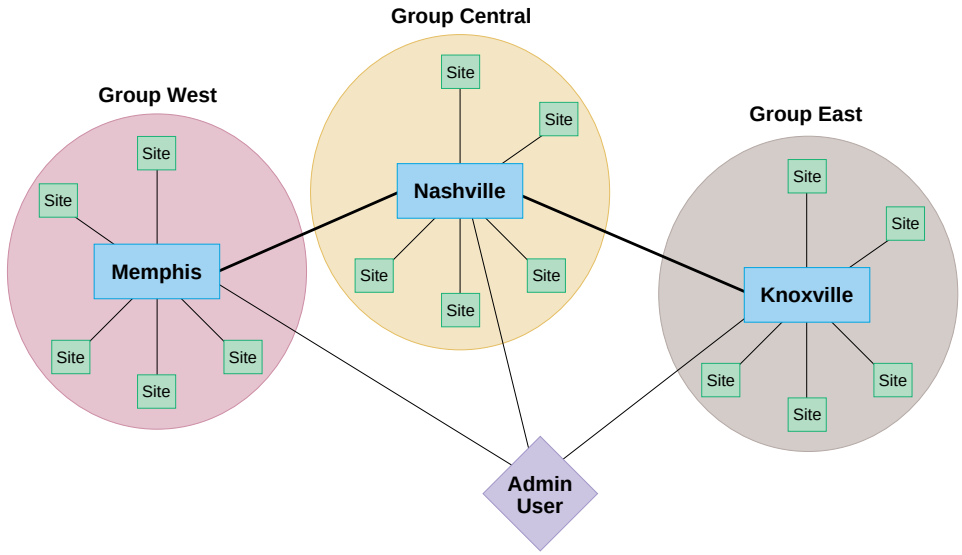
- connection groups
- sites and systems
- circuits (also known as lines)
- network protocol views

As shown below, an SFVRA-CFG network is composed of multiple sites that are attached via WAN circuits.



Through configuration, the SFVRA-CFG network can be subdivided into connection groups. These are groups of sites that can communicate with each other. Within each group a star network is normally defined. This means that there is one designated central site, and the rest of the sites in the group are considered “Remotes.”

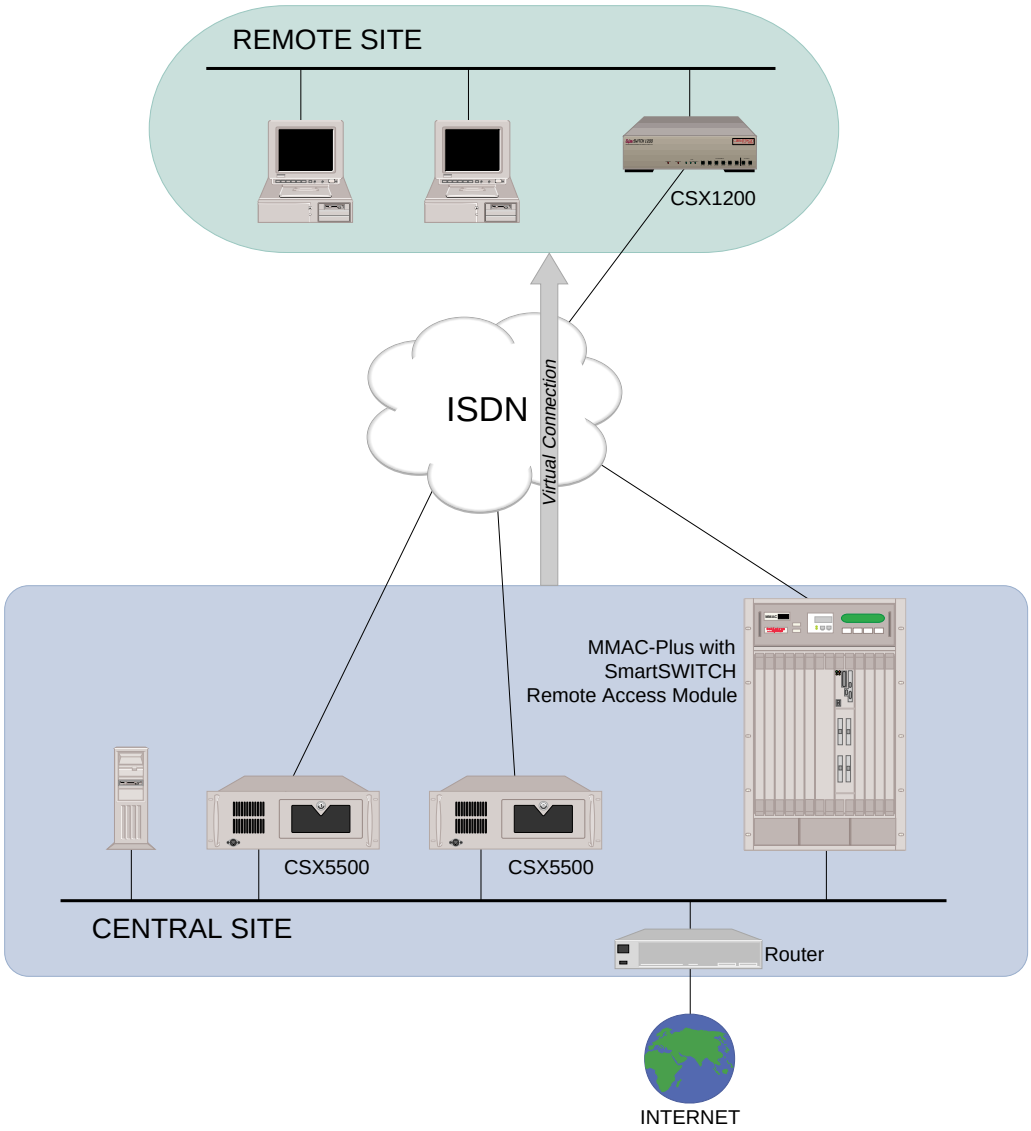
The following graphic illustrates the connection group concept.



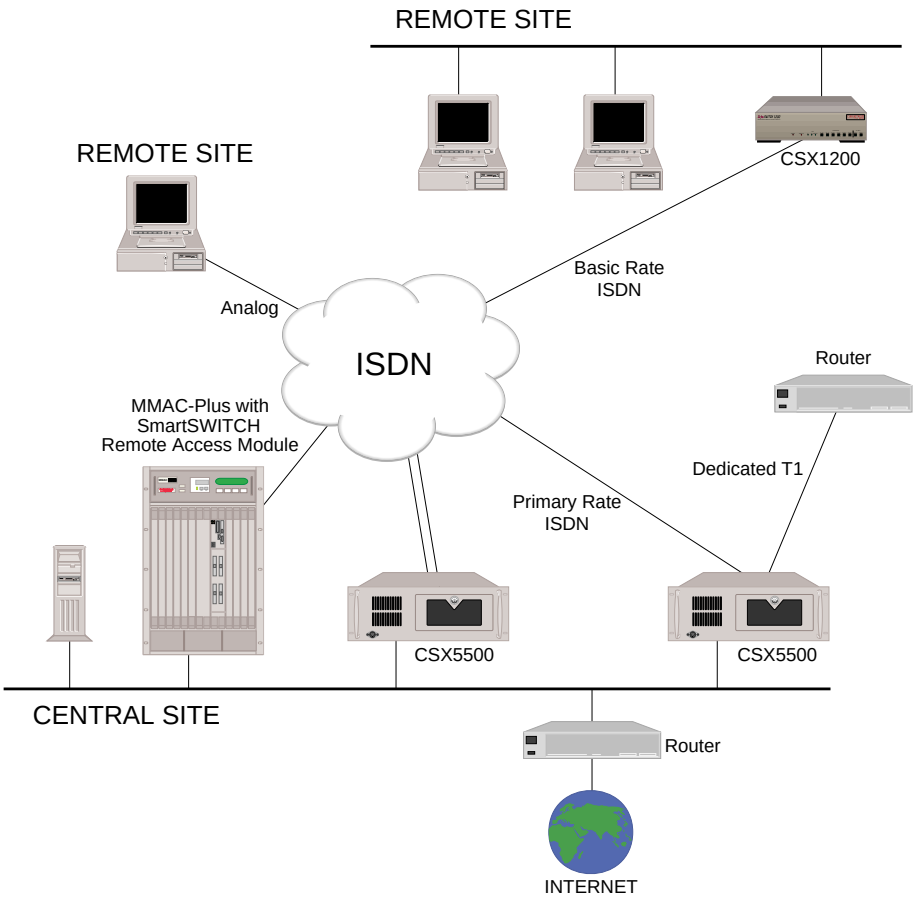
A site can have one or more systems. The systems are normally viewed as one system by other sites. This means that they can share a device authentication system name and authentication password / secret. They may optionally be connected to a multi-line hunt group. In a hunt group, all systems can share one phone number.

A system is a communication device that implements PPP (Point-to-Point Protocol) or Combinet Proprietary Protocol (CPP). It can be a communicating host (such as a PC with a modem) or a remote LAN with an attached bridge or router.

The following graphic illustrates possible site configurations and a mapping of the sites' physical and virtual connectivity.



Two sites can communicate by one or more connections that use circuits. A connection between two systems uses circuits at each end, one attached to each system. The graphic below illustrates the variety of circuits that can be used in an SFVRA-CFG network.



In addition to defining the physical topology of the network, the administrator also defines the virtual topology for each major network protocol. There is a separate protocol view for IP, IPX, and AppleTalk.

The SFVRA-CFG captures the definition of each subnet and segment, and how each system interfaces to it. This helps to generate all systems' configurations as well as any routing tables that are needed.

INTEROPERABILITY OVERVIEW

Interoperability is the ability to operate and exchange information in a heterogeneous network. SFVRA-CFG supports interoperability with many different remote devices over ISDN.

INTEROPERABILITY PROTOCOLS

In order to communicate with various remote devices over ISDN, the SFVRA-CFG must identify the device type and the line protocol it is using.

The line protocols supported are:

- Combinet Proprietary Protocol (CPP) Ethernet Frames
- Point-to-Point Protocol (PPP) Encapsulation for IP Datagrams

The PPP protocols supported are:

- LCP (Link Control Protocol)
- MLP (Multilink Protocol)
- Authentication Protocols
  - CHAP (Challenge Handshake Authentication Protocol)
  - PAP (Password Authentication Protocol)
- NCP (Network Control Protocols)
  - IPCP (Internet Protocol Control Protocol for TCP / IP)
  - IPXCP (Internetwork Packet Exchange Control Protocol for IPX)
  - BCP (Bridge Control Protocol for bridges)
  - ATCP (AppleTalk Control Protocol for AppleTalk Routing)
- CCP (Compression Control Protocol)

INTEROPERABILITY DEVICES

The remote devices that connect to Cabletron's CyberSWITCH or SmartSwitch Remote Access Module can be classified into three types:

- MAC Layer Bridges (PPP or HDLC)
- IP Host Devices (PPP)
- IP Router Devices (PPP)

MAC layer bridges connect to the Cabletron systems using either HDLC or PPP.

IP Host devices are single workstations or PCs that connect to the Cabletron systems at the IP network layer. These devices use PPP to communicate with the systems.

IP router devices are single devices that represent many other IP hosts and routers to the Cabletron systems. They must use the CHAP or PAP protocol to identify themselves to the system. IP routers usually provide IP network address information at connection time (and use PPP to send user data to the Cabletron systems).

SYSTEM COMPONENTS

The major components of SFVRA-CFG network are:

- *SFVRA-CFG Database*
  The storage vessel for network information. It is built on a either MS SQL Server, version 6.5 or later, or using Microsoft Access.

- *SFVRA-CFG Application*
  The interface to the SFVRA-CFG database.

- *Open Database Connectivity (ODBC)*
  An ODBC software driver that connects the SFVRA-CFG application with the SFVRA-CFG database.

ISDN NETWORK DEVICES

The SFVRA-CFG provides a centralized configuration / maintenance function for ISDN networks. The network devices can be separated into the following categories:

- ISDN routers
- remote ISDN bridge devices
- PC based terminal adapters
- ISDN enabled workstations

The SFVRA-CFG generates configuration files for the following Cabletron CyberSWITCH ISDN routers and SmartSwitch Remote Access Modules:

- 9W006
- 9W007
- CSX150
- CSX1000
- CSX1200
- CSX5500
- CSX6000
- CSX7000

These configuration files describe the CyberSWITCH / module and the devices that they connect to. Other types of ISDN routers may also be configured in a network. However, configuration files are not generated for these devices; the only information configured for these devices is the information that the CyberSWITCH / module requires.

Typical remote ISDN bridges provide one Ethernet port and one Basic Rate ISDN port. The Basic Rate port is connected to the switched digital network and is used to make connections to an ISDN router. The Ethernet port is used to connect to a remote LAN. The remote bridge device sends Ethernet frames from devices on the remote LAN over the switched network.

PC-based terminal adapters connect to a remote personal computer and use the switched digital network to connect to an ISDN router. The terminal adapter sends network protocol specific frames from the host PC device over the switched network.

Workstation-based terminal adapters connect to a workstation and use the switched digital network to connect to an ISDN router. The terminal adapter sends network protocol specific frames from the workstation over the switched network.

SYSTEM REQUIREMENTS

To ensure reliable service and optimal performance, your system should meet certain physical requirements. This section identifies components of an ideal hardware system on which to run SFVRA-CFG. Note that the SFVRA-CFG application runs optimally on the SFVRA-CFG database PC.

SFVRA-CFG'S DATABASE PC REQUIREMENTS

The following requirements apply only if using MS SQL Server. For optimal performance, we recommend:

- 100-200 MHz Pentium™ PC
- 32 MB RAM
- 200 MB free disk space (includes database)
- Windows NT 4.0
- Microsoft SQL Server 6.5 or above with SQL Server 32-bit ODBC driver
- Local network connection to managed systems
- Keyboard, mouse, and monitor

SFVRA-CFG'S APPLICATION PC REQUIREMENTS

- 100-200 MHz Pentium™ PC
- 32 MB RAM
- 15 MB free disk space
- Network connection to Microsoft SQL Server
- Windows 95 or Windows NT
- SQL Server or MS Access 32-bit ODBC driver
- Keyboard, mouse, and color monitor

SYSTEM INSTALLATION

The SFVRA-CFG consists of two components: the SFVRA-CFG Database that uses either MS SQL Server or MS Access; and the SFVRA-CFG application, which is the user interface to the database. You also need an Open Database Connectivity (ODBC) software driver to connect these two components.

This chapter provides instructions for installing the SFVRA-CFG system, and we also include instructions for installing the Adobe Acrobat Reader. You will need this reader to view the SFVRA-CFG user documentation.

INSTALLING THE SFVRA-CFG SYSTEM

As noted above, the SFVRA-CFG can operate with one of two databases: The MS SQL Server or MS Access. Installation instructions vary depending on the intended database. Instructions for each method follow.

INSTALLING WHEN USING MS SQL SERVER

When Using MS SQL Server as a database, you must perform the following steps to install the SFVRA-CFG system.

1. Install the MS SQL Server
2. Install the ODBC Driver Pack 3.0
3. Install the SFVRA-CFG Software
4. Install the SFVRA-CFG Database

The following sections include instructions for performing each step.

INSTALLING THE MS SQL SERVER

Install the SQL Server according to the manufacturer's instructions. Ensure that the MS SQL Server Service is running from the Start Menu \ Programs \ Microsoft SQL Server 6.5. Select SQL Service Manager and verify that the MS SQL Server Service is running. If it is not, select to start the service.

INSTALLING THE ODBC DRIVE PACK 3.0

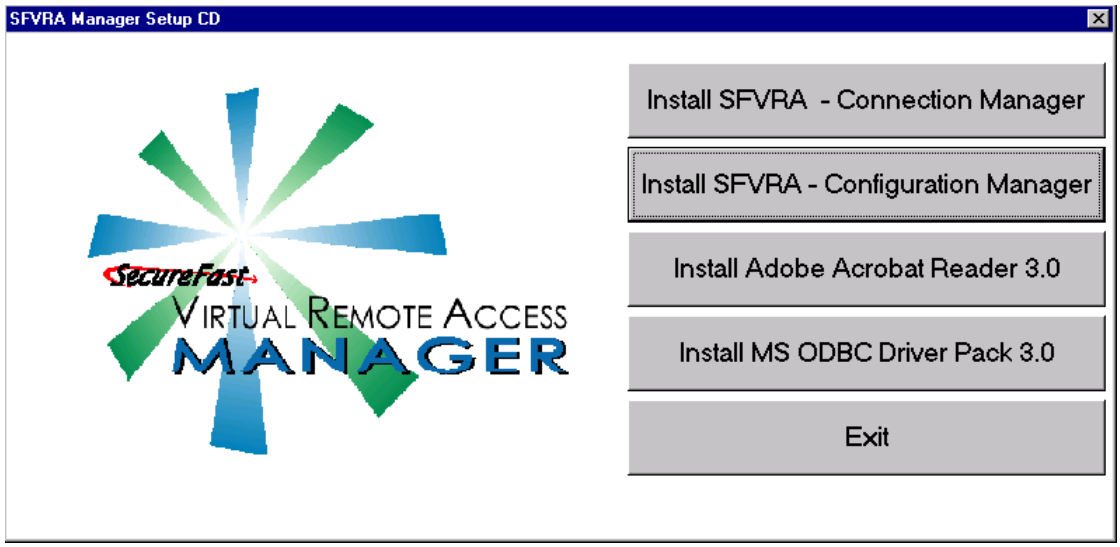
The ODBC hides the type of server, the location of the server, and the network protocol used to access the server from the application. This is an important feature; it gives the administrator the ability to control exactly how the database is being used. DBMS vendors usually provide ODBC

drivers that are specific to that type of database. SFVRA-CFG requires the use of a 32-bit ODBC driver.

Complete the following ODBC set-up on the device that will run the SFVRA-CFG application and on the device containing the MS SQL Server. As noted above, the ODBC will allow you to connect to the SFVRA-CFG database.

1. Close any active applications.

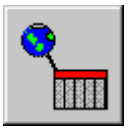
2. Insert the SFVRA Manager CD into the CD-ROM drive. If, as is usually the case, your CD-ROM is setup for AutoPlay, the following screen will automatically load:



   To manually load the above screen, select *Run* from the Start Menu. Enter *<CD-ROM drive>:\SCCD.EXE* as the program to open, then select *OK*.

3. From the initial install shield screen (shown above) click *Install ODBC Drive Pack 3.0*.

4. When prompted, choose the *Complete Install* option.

5. If installation fails, repeat the above steps, however, choose the *Custom*  option instead of *Complete Install*.
   a. Ensure that *SQL Server* and *ODBC components* are selected.
   b. Deselect *Desktop Drivers* and *Oracle* by clicking in the respective boxes.

6. If the Data Sources window is displayed during the installation of the ODBC Driver Pack select to *add* a datasource; otherwise, once the installation of the ODBC Driver Pack completes, select 32 bit ODBC from the Control Panel and select to *add* a data source.

7. Select the *SQL Server driver*. Click *OK*.

8. Enter *SFVRACFG* for the Data Source Name.

9. For *Server*, select the device on which the SQL server was installed.

10. Click *Options*. Enter *SFVRACFG* for the *Database Name*. Deselect *Generate Stored Procedure for Prepared Statement*. Click *OK*.

11. Click *Close*.

INSTALLING THE SFVRA-CFG SOFTWARE

SFVRA-CFG software must be installed on the system containing the SFVRA-CFG Database as well as on any system that runs the SFVRA-CFG application. During software installation, you will be given the option of installing:

- Program and Help Files
- SFVRA-CFG Database Setup Utility
- Documentation

You may install all components on one system if you wish to run the SFVRA-CFG application on the system containing the MS SQL Server.

Install SFVRA-CFG software using the following steps:

1. Ensure that ODBC setup has been performed on the systems.

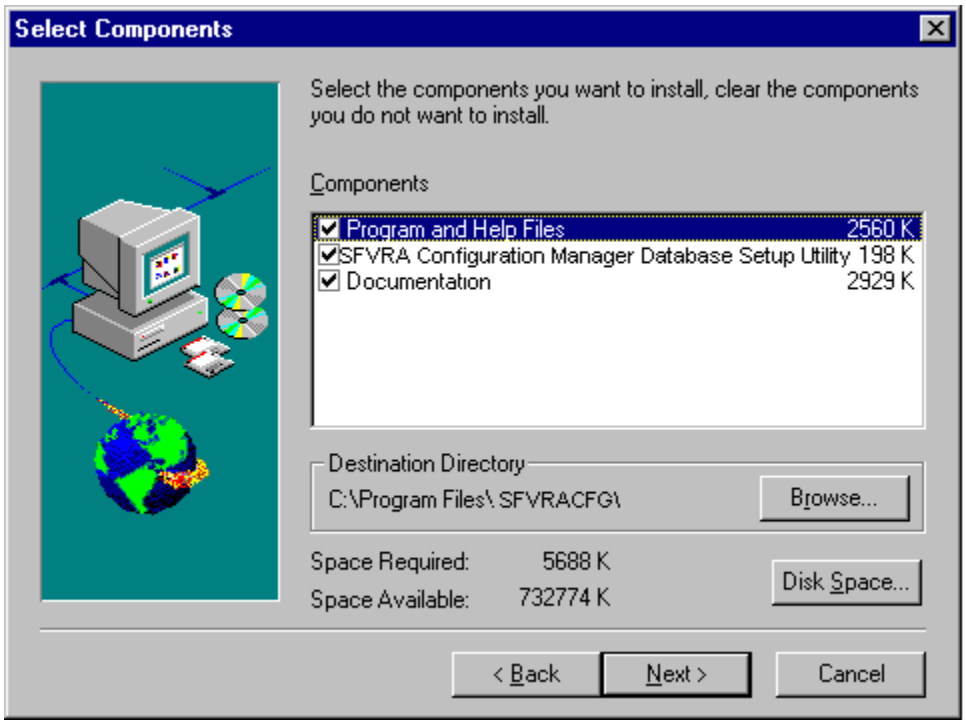
2. Close any active applications.

3. Insert the SFVRA Manager CD into the CD-ROM drive. If, as is usually the case, your CD-ROM is setup for AutoPlay, the initial installation screen will be displayed.

   To manually load the screen, select *Run* from the Start Menu. Enter *<CD-ROM drive>:\SCCD.EXE* as the program to open, then select *OK*.

4. From the displayed screen, select which SFVRA-CFG components you want to install. Click on *Install SFVRA Configuration Manager*.

5. The following screen will be displayed, allowing you to select which SFVRA-CFG components you want to install. Make sure a check appears next to the components you wish to install.


Select Components
Select the components you want to install, clear the components you do not want to install.
Components
Program and Help Files 2560 K
SFVRA Configuration Manager Database Setup Utility 198 K
Documentation 2929 K
Destination Directory
C:\Program Files\ SFVRACFG\
Browse...
Space Required: 5688 K
Space Available: 732774 K
Disk Space...
< Back
Next >
Cancel

Note: The SFVRA-CFG Database Setup Utility should only be installed on the PC running the MS SQL Server.

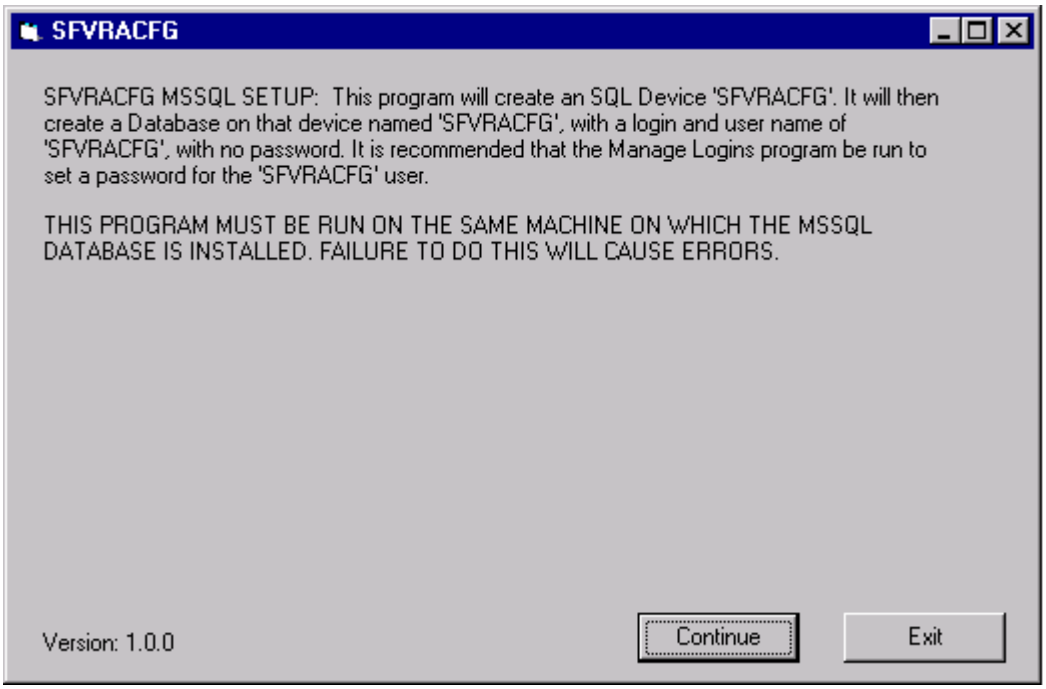
6. Follow onscreen instructions to complete the installation.

INSTALLING THE SFVRA-CFG DATABASE

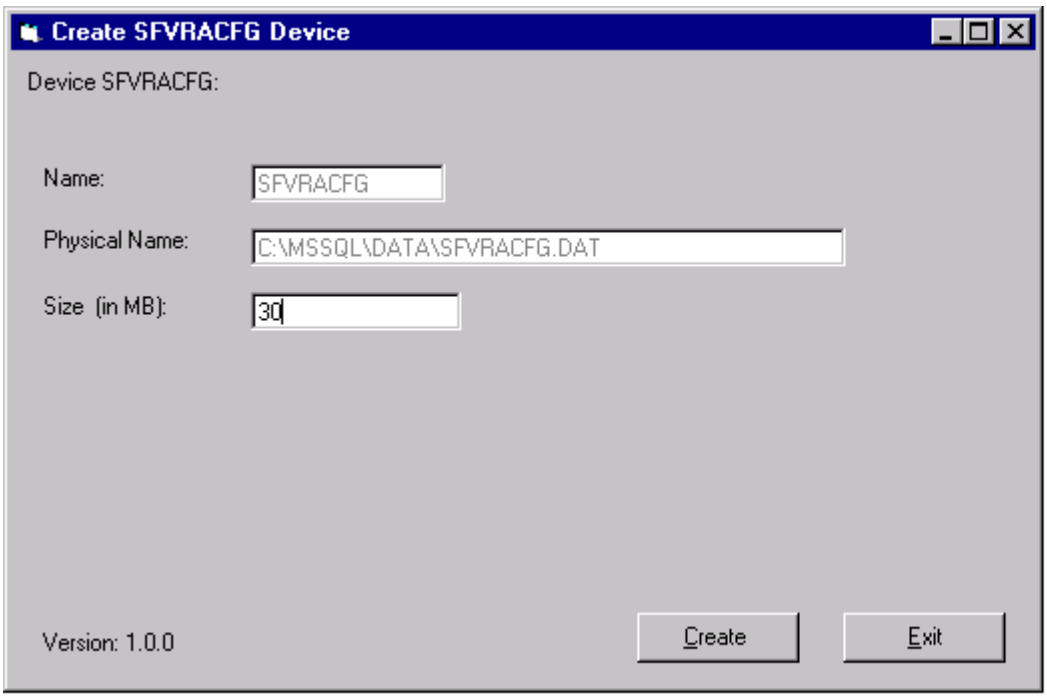
The SFVRA-CFG uses Microsoft (MS) SQL Server (6.5 or later) for its database. Install this database on a Windows NT device.

1. Create the SFVRACFG database.
   a. The SFVRACFG database is created by the SFVRA-CFG Database Setup Utility. You may choose to run this utility when installing SFVRA-CFG software. If you choose not to run the utility while installing the software you may start the utility after completing the software installation. To do this, from the Start menu\Programs\SFVRA Configuration Manager, select *SFVRA-CFG Database Setup*.
   b. Enter the *sa* password, if necessary, and click OK. The SQL Setup program executes.

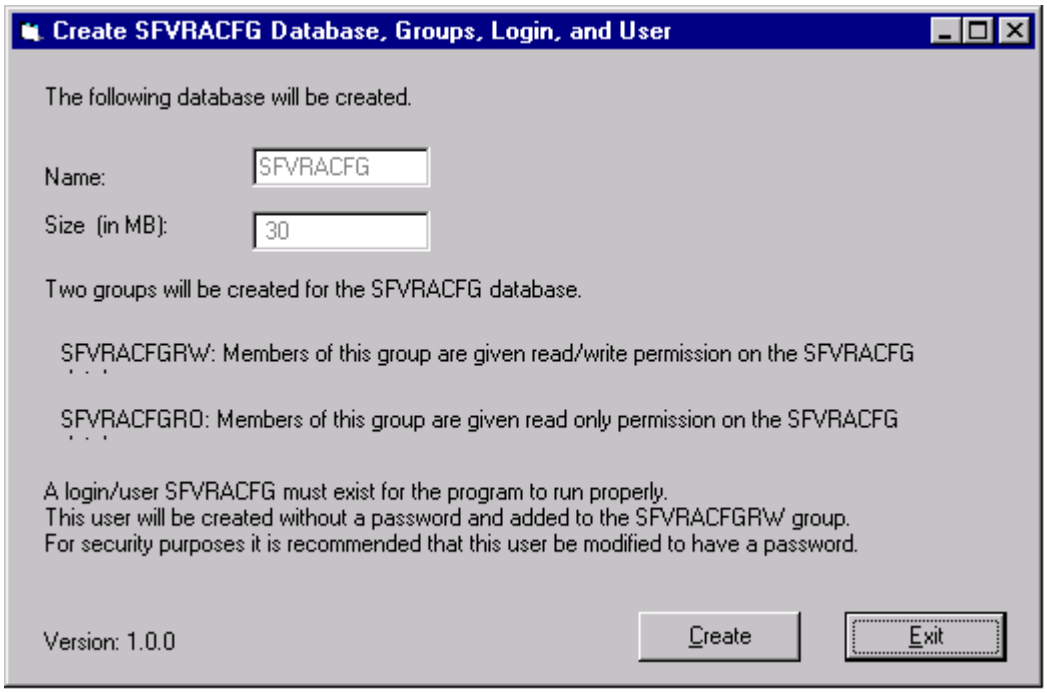
c. The SQL Setup program first creates the SFVRACFG Device. The following screen appears:


SFVRACFG
SFVRACFG MSSQL SETUP: This program will create an SQL Device 'SFVRACFG'. It will then create a Database on that device named 'SFVRACFG', with a login and user name of 'SFVRACFG', with no password. It is recommended that the Manage Logins program be run to set a password for the 'SFVRACFG' user.
THIS PROGRAM MUST BE RUN ON THE SAME MACHINE ON WHICH THE MSSQL DATABASE IS INSTALLED. FAILURE TO DO THIS WILL CAUSE ERRORS.
Version: 1.0.0
Continue
Exit

d. Click on *Continue*. Note that on the resulting screen, the Size (in MB) is blank. As entered below, we recommend specifying the device size of at least 30 MB.



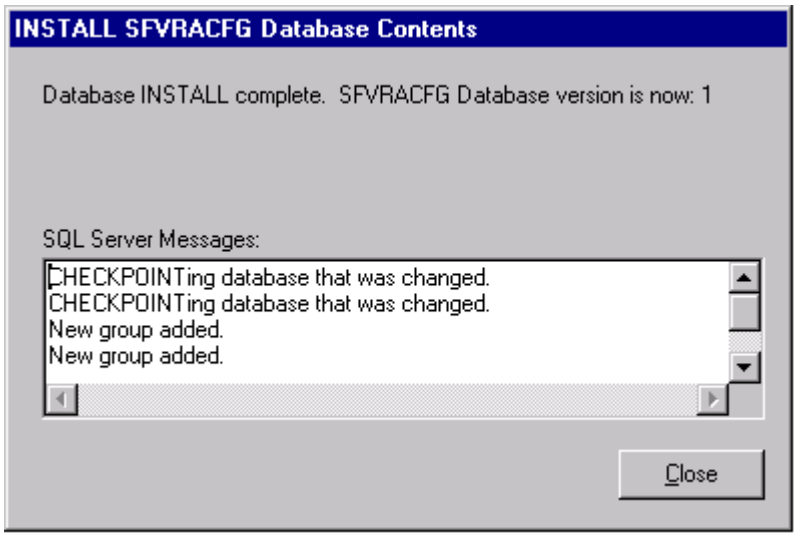
2. Once the SFVRACFG Device has been created, the SQL Setup will create the SFVRA-CFG database, groups, and the SFVRACFG login ID. A screen similar to the following appears:


Create SFVRACFG Database, Groups, Login, and User
The following database will be created.
Name:
SFVRACFG
Size (in MB):
30
Two groups will be created for the SFVRACFG database.
SFVRACFGRW: Members of this group are given read/write permission on the SFVRACFG
SFVRACFGRO: Members of this group are given read only permission on the SFVRACFG
A login/user SFVRACFG must exist for the program to run properly.
This user will be created without a password and added to the SFVRACFGRW group.
For security purposes it is recommended that this user be modified to have a password.
Version: 1.0.0
Create
Exit

Click *Create*.

3. After the SFVRA-CFG Database has been successfully created, the SQL Setup will create database tables. Click *OK*. This procedure may take several minutes (the SQL Setup runs an ISQL script).

4. When the SQL Setup program has finished, a screen similar to the following is displayed.


INSTALL SFVRACFG Database Contents
Database INSTALL complete. SFVRACFG Database version is now: 1
SQL Server Messages:
CHECKPOINTing database that was changed.
CHECKPOINTing database that was changed.
New group added.
New group added.
Close

Ensure that no error messages are listed in the SQL Server Messages dialog. Click *Close*.

Login Accounts

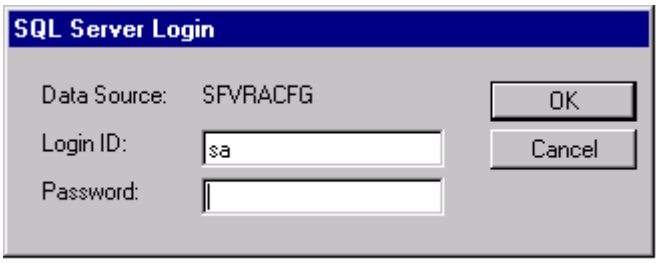
Different login accounts may be created based on who is operating the SFVRA-CFG. For instance, the system administrator will need to *make changes* to the database to update network information, whereas a general user may need to just *view* the configuration information in the database. Therefore, the system administrator will need to have Read / Write access to the database; the general user will only need to have Read access. The Manage Logins program allows you to create different Login IDs.

Only the system administrator may add new logins or modify existing login. The system administrator login is *sa*. All other accounts only have the ability to view the Database Access of the other accounts.

The Login ID SFVRACFG is created when the SFVRA-CFG database is created. This account is created with Read / Write access and with no password. We recommend that a password is configured for this account, and any accounts created thereafter.

To create or modify a login account:

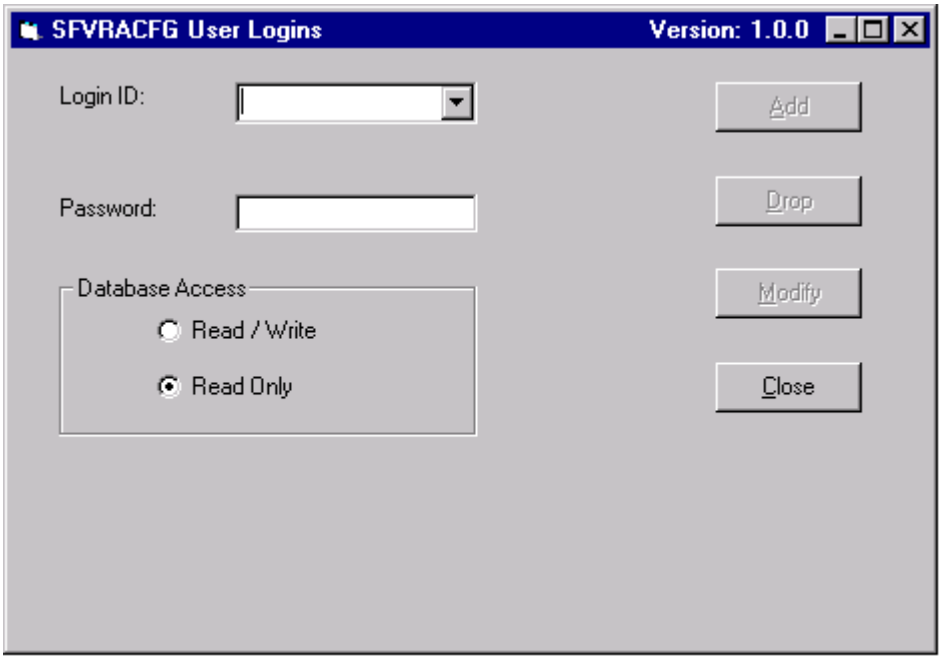
1. From the Start menu \ Programs \ SFVRA Configuration Manager, select *SC Manage Logins*. A screen similar to the following will be displayed:



2. Login as *sa* (system administrator) as shown above.

3. Enter the *Password* for login *sa* (if applicable).

4. Click on *OK*. The following screen will be displayed:



5. Select the *Login ID* you wish to modify, or select <*New Login*> to create a new account.

6. Enter a *Password*. You will later be prompted to confirm the password.

7. Select the type of *Database Access* (choices are *Read/Write* or *Read Only*).

8. Click *Add* for new accounts, or click *Modify* for previously existing accounts. *Drop* removes the account from the database.

9. Click *Close*.

INSTALLING WHEN USING MS ACCESS

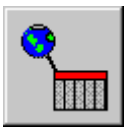
When Using MS Access as a database, you must perform the following steps to install the SFVRA-CFG system.

1. Install the SFVRA-CFG Software (follow the same software installation instructions provided for installation using MS SQL Server).

2. Install the ODBC Drive Pack 3.0.

INSTALLING THE ODBC DRIVE PACK 3.0

Complete the following ODBC set-up on the device that will run the SFVRA-CFG application and on the device containing MS Access. Note that you must already have a Microsoft application (such as MS Word, MS Office, etc.) on your device. The ODBC will allow you to connect to the SFVRA-CFG database.

1. From the initial install shield screen click *Install ODBC Drive Pack 3.0*.
2. When prompted, choose the *Complete Install* option.
3. If installation fails, repeat the above steps, however, choose the *Custom*  option instead of *Complete Install*.
   a. Select *Desktop Drivers* and press *Change Option*.
      - Select *MS Access Driver*, *Engine components*, and *Help Files*.
      - Deselect all other drivers and press *OK*.
   b. Deselect *SQL Server* and *Oracle* by clicking in the respective boxes.
   c. Ensure that *ODBC components* is selected and press *Continue*.
4. If the Data Sources window is displayed during the installation of the ODBC Driver Pack select to *add* a datasource; otherwise, once the installation of the ODBC Driver Pack completes, select 32 bit ODBC from the Control Panel and select to *add* a data source.
5. Select the *MS Access driver*. Click *OK*.
6. Enter *SFVRACFG* for the Data Source Name.
7. Select *scfgper.mdb* as the database. The path to this database is:
   `C:\program files\sfvracfg\program\scfgper.mdb.`

INSTALLING ADOBE ACROBAT READER

To review or print the SFVRA-CFG documentation (User's Guide and Parse Wizard Guide), you will need Adobe Acrobat Reader. We have included the Reader setup utility on this CD for those of you who do not already have a version of Reader.

To install Adobe Acrobat Reader:

1. Close any active applications.
2. Insert the SFVRA Manager CD into the CD-ROM drive. If, as is usually the case, your CD-ROM is setup for AutoPlay, the initial installation screen will be displayed.
3. On the SFVRA Manager initial installation screen, click on *Install Adobe Acrobat Reader 3.0*.
4. Follow the onscreen instructions to complete the installation.

To view the SFVRA-CFG documentation:
From the Start menu\Programs\SFVRA Configuration Manager, select SFVRACFG Documentation.

USING THE SFVRA-CFG APPLICATION

OVERVIEW

This chapter includes the following sections:

- SFVRA-CFG Scenarios
  The SFVRA-CFG application proves useful in a variety of network scenarios. This section provides a description and instructions for common scenarios.

- Starting the SFVRA-CFG
  This section provides instructions for starting up the SFVRA-CFG application.

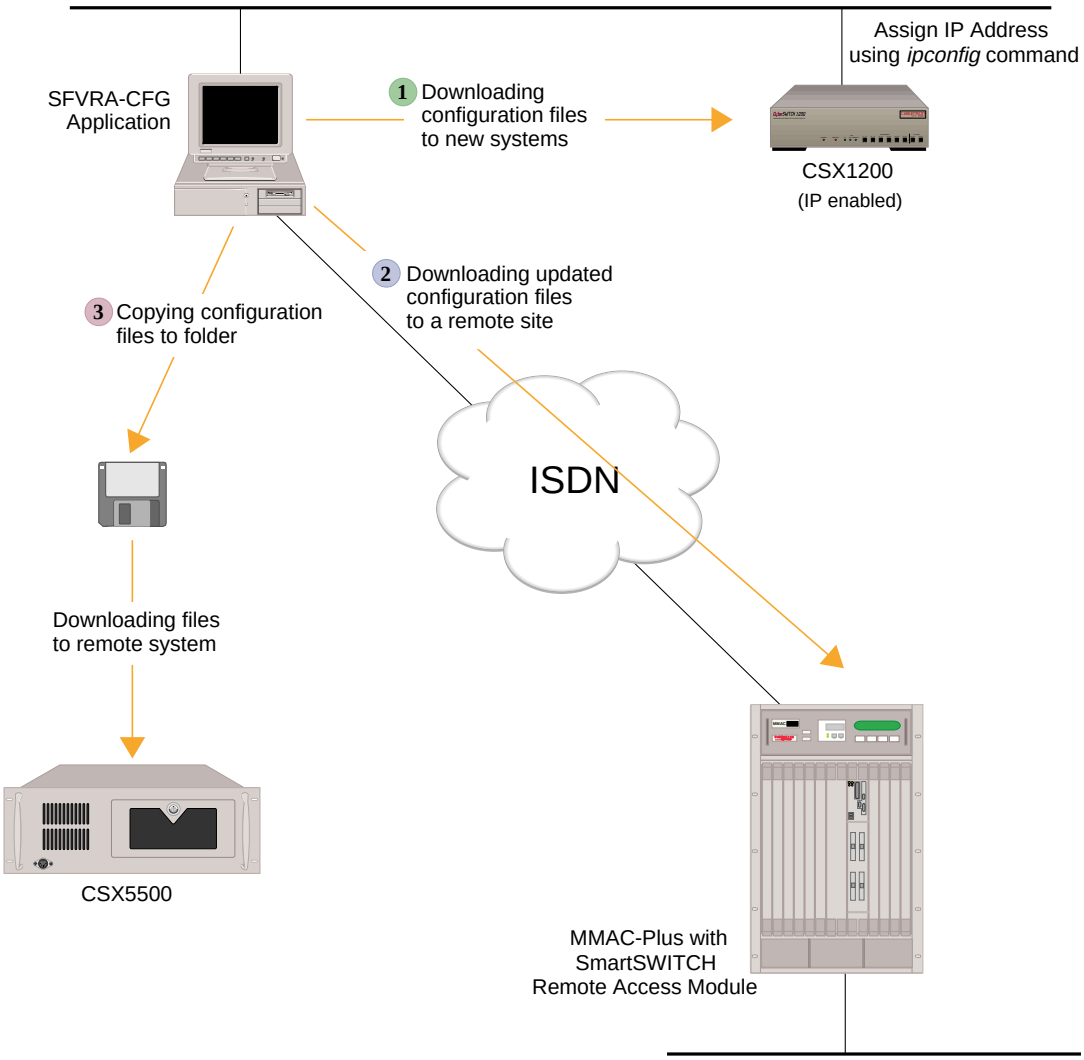
- Configuration Building Blocks
  When using the SFVRA-CFG application, you start by configuring basic information, such as product codes, and then use that information while progressing through other configuration steps. This section steps you through the SFVRA-CFG's configuration building blocks.

- Using the SFVRA-CFG Menus
  This section provides a brief description of common SFVRA-CFG menu buttons (*Add*, *Select*, *Delete*, *Refresh*, *Close*).

- System Messages
  This section briefly discusses system messages you might see while using the SFVRA-CFG application.

SFVRA-CFG CONFIGURATION SCENARIOS

SFVRA-CFG is a tool that allows you to centrally create configuration files for CyberSWITCH systems or SmartSwitch 9W006/9W007 modules, then download those configuration files to the systems or modules. As illustrated by the following graphic, this tool can be used in a variety of configuration situations. This tool can be used to configure all systems in a new network (see scenario #1); it can be used to download updated configuration files to a system in an established network (see scenario #2); it can also be used to copy updated configuration files to a designated folder, perhaps on a diskette, which could then be delivered to a site and used to update a system's configuration files (see scenario #3).



Refer to the section below that pertains to your configuration situation.

NEW NETWORK CONFIGURATION

SFVRA-CFG is a valuable tool when setting up a new network. At a central location, you can use SFVRA-CFG to configure new CyberSWITCH systems or SmartSwitch Remote Access Modules, one at a time, then ship them to their remote sites.

The steps for configuring a new network are:

1. Access the system using a device running a terminal application. Connect one end of the supplied null modem cable to the RS232 console port on the module or CyberSWITCH, and the other end of the cable to the communication port on the device. On the device you must then execute a communication package to emulate a terminal (VT100).

Use the following default values for your communication package:

Baud rate	9600
Parity	None
Data bits	8
Stop bits	1
Duplex	Full

2. You should then have a connection to the module or CyberSWITCH. You will be prompted for a login ID and the initial password. Enter *admin* for both.

3. You will now see the system prompt. We recommend that you select a new password. To do this, enter the following command at the system prompt then follow the onscreen directions:
   pswd

4. To assign the module's new IP address, enter the following command at the system prompt:
   ipconfig

   Then as prompted, enter:
   - the system's IP address
   - the required subnet mask
   - for the system's default route, enter the IP address of the system's default gateway (enter 0 if there is no default route)

   Follow the instructions to restart the module so that the configuration changes will take effect.

5. Using SFVRA-CFG, configure the system's or module's configuration information.

6. Generate then download the configuration files from the SFVRA-CFG to the new system. Instructions for generating and downloading configuration files are located in *Exporting Configuration Files*.

7. When the download is complete, the system will automatically restart, making the configuration changes permanent.

8. The new system should now be configured and ready to be placed at its remote site. Remove the system from the LAN.

9. Repeat the above steps for each system.

UPDATES FOR AN ESTABLISHED NETWORK

Once you have an established network, you can use the SFVRA-CFG application to centrally update a system's configuration database files, then generate and download the updated configuration files from the SFVRA-CFG to the system. Instructions for generating and downloading configuration files are located in *Exporting Configuration Files*.

COPYING UPDATED FILES

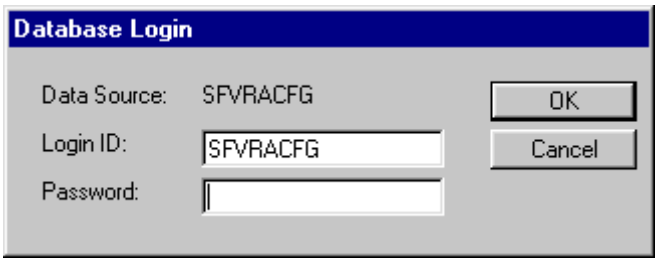
At times you may find it necessary to copy (as opposed to download) updated configuration files. For example, if a remote system's configuration files somehow become corrupted, you may not be

able to communicate with the system through its IP address. The SFVRA-CFG application would not be able to download new configuration files; it would not know where to download the files to. To solve this problem, you can use the SFVRA-CFG application to generate and copy updated configuration files from the SFVRA-CFG to a specified folder. (The folder can be designated to be on a diskette, or perhaps a server.) You can then copy the configuration files from the diskette (or the server) to the system. Instructions for generating and copying configuration files are located in *Exporting Configuration Files*.

STARTING THE SFVRA-CFG APPLICATION

To start the SFVRA-CFG:

1. Open the SFVRA-CFG application.
2. From the menu bar, click on *File* then click on *Connect*, or click on the toolbar.
3. A dialog box similar to the following will be displayed:



Note that the first time you use the SFVRA-CFG application, the login ID is set to SFVRACFG. If desired, you may edit this field to change the login ID.

4. If required, enter your password.
5. Click *OK*.

CONFIGURATION BUILDING BLOCKS

Using the SFVRA-CFG to enter configuration information is based on a building block concept. You start with basic information, then you build more information using that basic information.

You begin by building a product code table. A product code is a user-defined code that is associated with a particular product. For example, you could enter CSX1201 as a product code, and select CyberSWITCH 1201 as its associated product. Later, as you configure sites, you will use the product codes when adding systems to the sites.

Next, if your network uses any SFVRA Connection Managers, you will specify information about any SFVRA Connection Manager databases required. For each SFVRA database, you enter an SFVRA database location and the SFVRA database version that is running. Later, as you configure sites, you will select either *Local User Table* or *SFVRA* for the User Database. If you select SFVRA, you will also need to select the SFVRA database site. You will select this from the displayed list of previously configured SFVRA database locations.

After the tables are complete, you progressively configure the information that falls under the function menu — beginning with building site templates, then sites, circuits, connections groups, applicable protocol information (IP, IPX, or AppleTalk), and ending with any SNMP management groups.

A site template is a time-saving tool that allows you to configure a template of generic site information that can be used over and over for similar sites. Generic site information includes:

- Physical Resource Information
  Includes BRI, PRI, V.35, and RS232 information. When applicable, switch type and related information can also be entered.

- Site Options
  Allows you to enable / disable protocols (bridging, IP, IPX, AppleTalk). Also allows you to configure options such as SNMP, PPP, Call Control, and Default Line Protocol.

- Security Information
  Allows you to configure local user table settings (the type of security used — PAP, CHAP, bridge MAC address, or CLID), or if the site uses an SFVRA Manager, you can configure TCP port information. Configuring administrative session information is optional.

- Connections
  Allows you to specify how the site's systems will handle connections. For example, you can set up call restrictions for the site template.

After you have designed site templates, you are then ready to define specific sites. For each site you will enter various site properties (including the site template you wish to use for this site), optional contact information, and the systems associated with this site. You will need to select a product code for each system that you add to the site.

The next building block is the circuits. The circuits describe the physical WAN connections to each system. Circuit information includes line properties, and where applicable, data link and access information.

Through connection groups, you can logically group sites together. You can also select a central site for the group, creating a star configuration.

You also need to define any IP network subnets, IPX network segments, and / or AppleTalk network segments. This information provides IP and IPX interface information, and AppleTalk port information.

Finally, configure any SNMP Management Groups. These are a group of sites that can be collectively managed by an SNMP Manager.

Note that when changing or deleting information, you must work backwards, from the top layer of building blocks down. For example, you cannot delete a site if that site is included in other upper level configuration information, for instance, if it is included in a connection group. You must first delete the site from the connection group, then you may delete the site.

USING THE SFVRA-CFG MENUS

Many of the SFVRA-CFG menus share common menu buttons. This section provides a brief description of the following common buttons:

- *Add*
  Click on *Add* then follow onscreen instructions for adding the item. In some instances, you must complete the information on the initial menu screen, then click on *Add* before you will be able to enter information on any of the other related screens.

- *Select*
  To display more information for a line item (i.e., a particular connection), highlight the item you would like to select, then click on *Select*. To get the same results, you may also double click on the line item.

- *Duplicate*
  This menu option is only available for the *Product Code* menu and the *Site Templates* menu. This option allows you to duplicate an existing item, then make changes to the duplicate. For example, if you need two site templates that are very similar, you can completely configure one template, then duplicate the template and make the necessary changes for the second template. This is much more efficient than completely configuring both templates.

- *Delete*
  To delete a specific item, highlight the item, then click on *Delete*. Note that if you try to delete an item that is used elsewhere, you will see an error message. For example, if you try to delete a site that is part of a connection group, you will see an error message. You would need to first delete the site from the connection group, then you could delete the site.

- *Refresh*
  When the SFVRA-CFG displays information in windows, the information shown is a "snapshot." It is possible for changes to be made in one window of the SFVRA-CFG application which cause information displayed in another window to become out-of-date. To update open window snapshots, click on *Refresh*. The refresh option is available on all of the main SFVRA-CFG menus.

- *Close*
  Allows you to close the menu you are currently using. You will be alerted if there is required information that you have not yet entered.

SYSTEM MESSAGES

The system messages you see while using the SFVRA-CFG come from three sources: they are either generated by the SFVRA-CFG application, MS SQL Server, or MS Access.

The SFVRA-CFG's messages are usually self-explanatory, for example, if you try to download an update that you have not yet generated, you will see a message telling you just that.

To interpret an MS SQL Server generated message, refer to MS SQL Server documentation, such as the *MS SQL Server Administrator's Companion*.

To interpret an MS Access generated message, refer to MS Access documentation.

CONFIGURING TABLES

OVERVIEW

Before you begin configuring site and network specific information, you must first configure the product code table, and, if applicable, the SFVRA database table.

The product code table allows you to associate a user-defined code with a particular platform. For example, you could enter *CSX6000a* as a product code, and select *CyberSWITCH 6000* as its associated platform. Later, as you configure sites, you will use the product codes when adding systems to the sites.

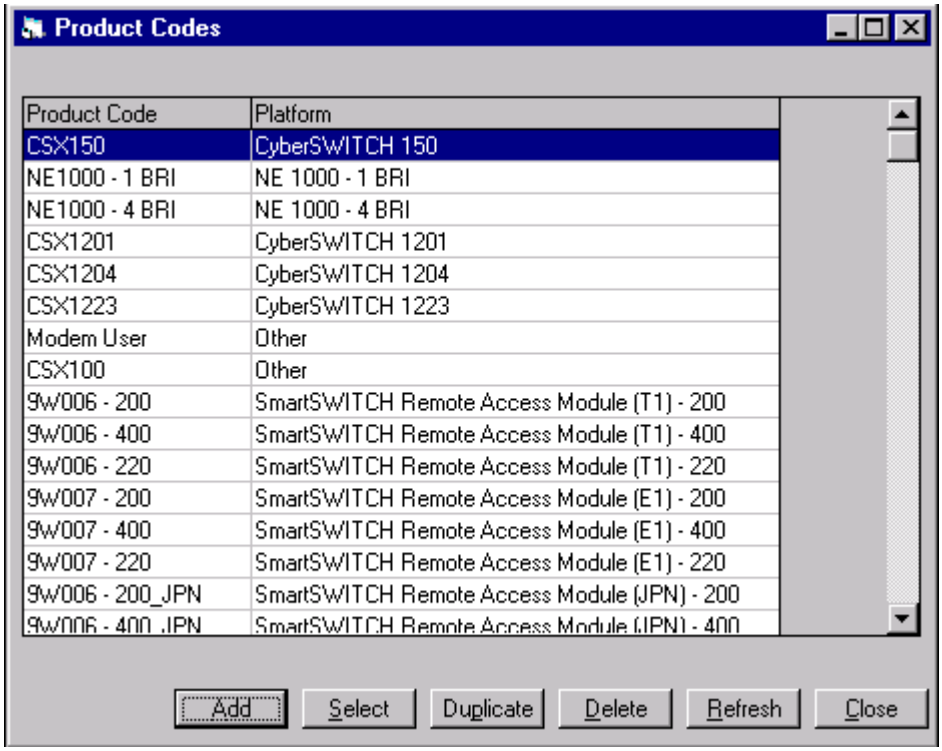
You only need to configure the SFVRA database table if your network uses an SFVRA Connection Manager for a user database. For each SFVRA table entry, you enter an SFVRA database site name and the SFVRA database version that is running. Later, as you configure sites, you will select either *Local User Table* or *SFVRA* for the User Database. If you select SFVRA, you will also need to select the SFVRA database site. This is selected from the displayed list of previously configured SFVRA database locations, which are part of the SFVRA database table.

This chapter provides instructions for:

- configuring the product code table
- configuring the SFVRA table

CONFIGURING THE PRODUCT CODE TABLE

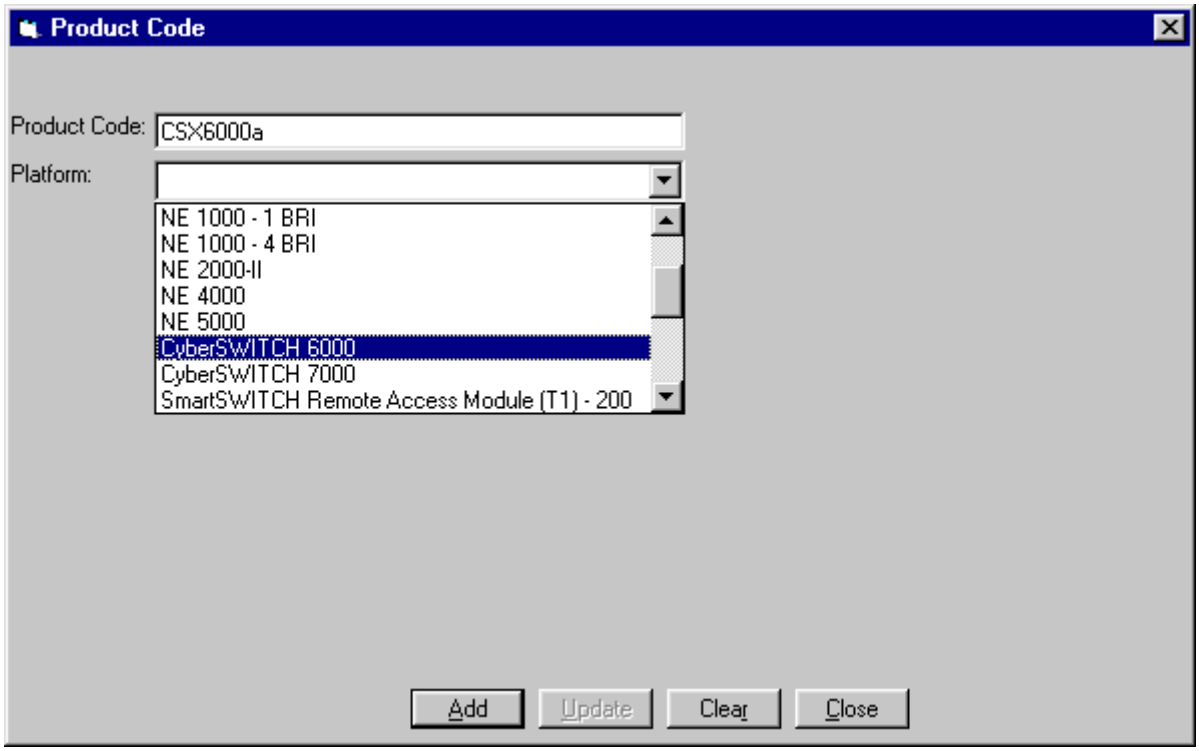
The product code table is preconfigured with basic codes. To add new product codes to the table click on *Tables* from the menu bar. From the resulting menu, click on *Product Codes*. The preliminary product code table will be displayed as shown below:



1. Click on *Add*.

2. Enter a user-defined *Product Code*. The product codes are tied to a specific platform.

   On the example screen shown below, we have entered *CSX6000a* for the product code. This will allow us to add more than one product code for the CyberSWITCH 6000 platform. This is useful if the network has CyberSWITCH 6000s with more than one adapter configuration. We can then give a separate product code, for example *CSX6000b*, to a CyberSWITCH 6000 with an adapter configuration different than that of *CSX6000a*.



3. Select the *Platform* you want associated with the product code (as shown above). If the platform is not a CyberSWITCH or an NE platform, select *Other*.

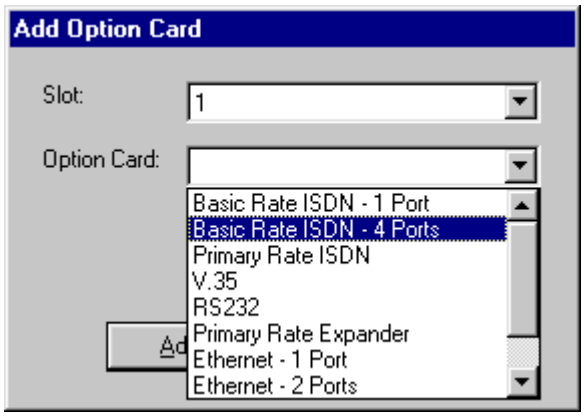
4. Click on *Add*.

5. If the platform you selected can have option cards (i.e., PC-based platforms) you will need to add the system's option cards to the product code table as described below.

   a. Click on *Add Option Card.*

   b. Select the *Slot* number the option card is installed in.

c. Select the *Option Card* type. In the example screen shown below, we are configuring a 4 port BRI option card to be in slot 1.



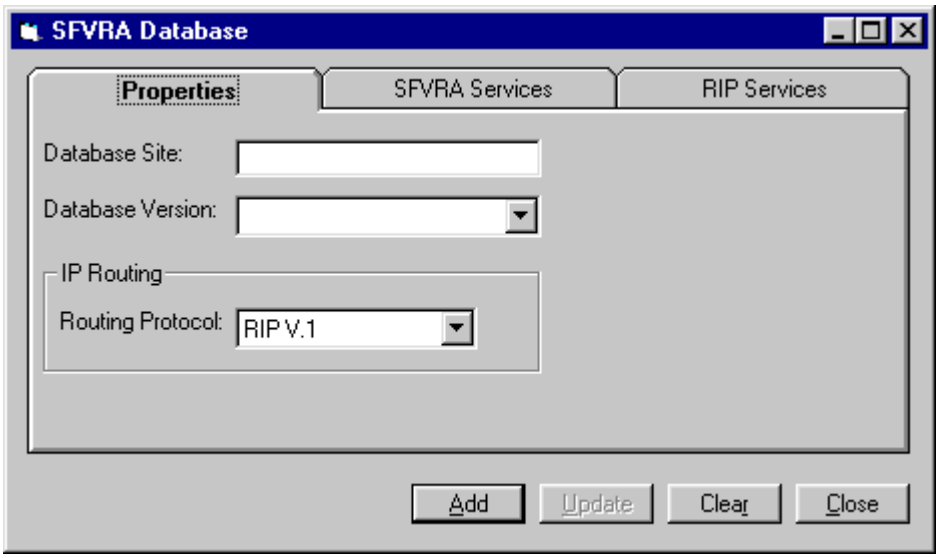
d. Click on *Add*. Repeat above steps for each option card.

6. Click on *Close* when finished adding table entries.

CONFIGURING THE SFVRA DATABASE TABLE

To add an SFVRA database to the table:

1. From the menu bar, click on *Tables.*
2. From the resulting menu, click on *SFVRA Databases*.
3. Click on *Add*. The following table will be displayed:



4. Configure the SFVRA Database *Properties.*

    a. Enter a user-defined name for the *Database Site.* Note that you must configure an ODBC Data Source Name for each SFVRA database site name you configure. This can be done through your device's Control Panel (use the instructions provided in *ODBC Setup*, substituting SFVRA information where needed).

    b. Select the SFVRA *Database Version*.

    c. Configure the SFVRA database site's *IP Routing* information: select the RIP *Routing Protocol* that the SFVRA Manager will use to route IP packets.

    d. Click on *Add.*

5. Click on the *SFVRA Services* tab. Use the resulting screen to configure the SFVRA services associated with this SFVRA database. SFVRA services perform remote user authentication and connection management functions for the SFVRA Manager.

    a. Click on *Add.*

    b. Enter the *IP Address* used by the RIP service to connect to the SFVRA service.

    c. Optional. Enter a *Description* of the SFVRA service. For example, you may wish to use the computer name or location where the SFVRA service is running.

    d. Click on *OK*. Repeat above steps to add any additional SFVRA services.

6. Click on the *RIP Services* tab. Use the resulting screen to configure the RIP services associated with this SFVRA database. The RIP service operates by advertising itself as a path to reach one or more remote subnets.

    a. Click on *Add.*

    b. Enter the *Computer Name* for the Windows NT system on which the RIP service runs. This may be found on the Windows NT system by selecting Network from the Control Panel.

    c. Optional. Enter the *Description* for the RIP service. For example, you may wish to use the computer name or the location where the RIP service is running.

    d. Select a *Connection Group* for which the RIP service will advertise routes.

        Note: Multiple groups may be assigned to one RIP service, however, each group must be configured with the RIP service as a separate entry.

    e. Click on *OK*. Repeat above steps to add any additional RIP services.

7. Repeat steps 3 through 6 to add additional SFVRA databases to the table.

8. Click on *Close* when finished adding table entries.

CONFIGURING SITE TEMPLATES

OVERVIEW

A site template is a time-saving tool, allowing you to configure a template of basic site information that can be used over and over to configure similar sites. Basic site information includes:

- Physical Resources
  Includes BRI, PRI, V.35, RS232, and Digital Modem information. When applicable, switch type and related information is also entered.

- Options
  Allows you to enable protocols that will be used by the site (bridging, IP, IPX, AppleTalk). Also allows you to configure options such as SNMP, PPP, Call Control, and Default Line Protocol.

- Security
  Allows you to configure local user table settings (i.e., the type of security used — PAP, CHAP, bridge MAC address, or CLID), or if the site uses an SFVRA Manager, you can configure TCP port information. Configuring administrative session information is optional.

- Connections
  Allows you to specify how the site will handle connections. Connection information is grouped into the following categories: authentication, restrictions, access, and protocols.

Note that many parameters configured in a site template are used to initialize the configuration of a site when the site is added. These parameters may be overridden for a particular site or for particular items added to a site. There are also some parameters that can only be configured in the template; they are not available at the system level. The following site template parameters *can not* be overridden:

- under *Physical Resources*
  all digital modem information

- under *Options*
  MAC Layer bridging: all information except enable / disable
  IPX: RIP / SAP max table entries
  AppleTalk: max route / zone table entries
  SNMP: all information
  PPP: all information
  Call Control: all information
  Default Line Protocol: all information

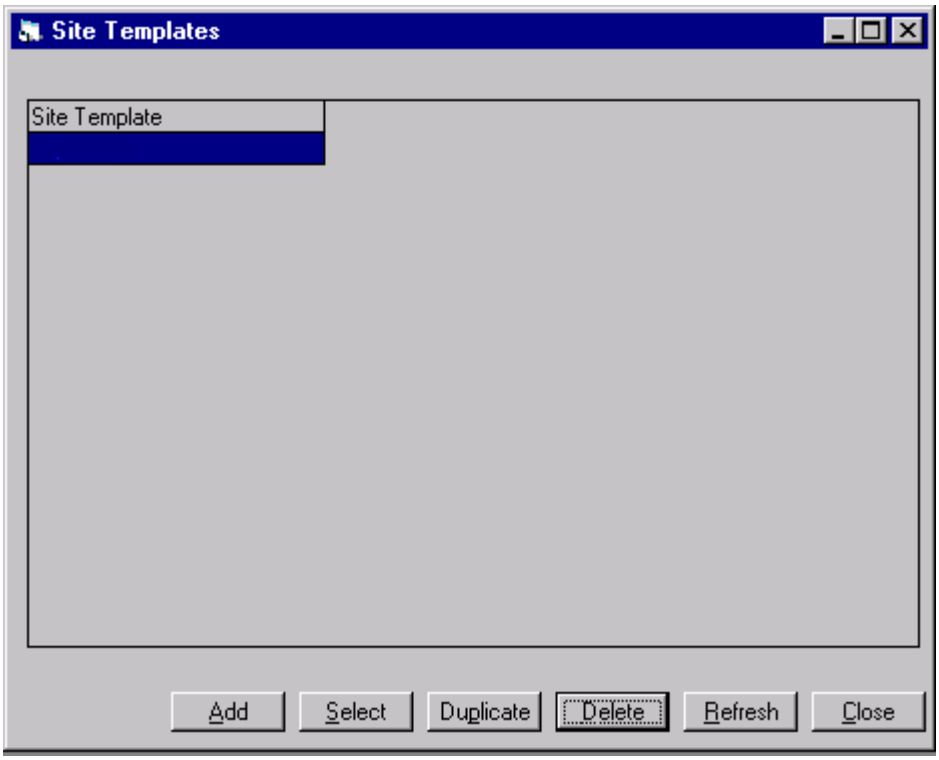
- under *Security*
  all information

If a site requires a different value for a parameter that can not be overridden, a new site template must be created for the site. The site template dialog box has a duplicate option that is very useful for this situation. You can create a duplicate site template, and make changes where necessary to the duplicate.

ADDING A SITE TEMPLATE

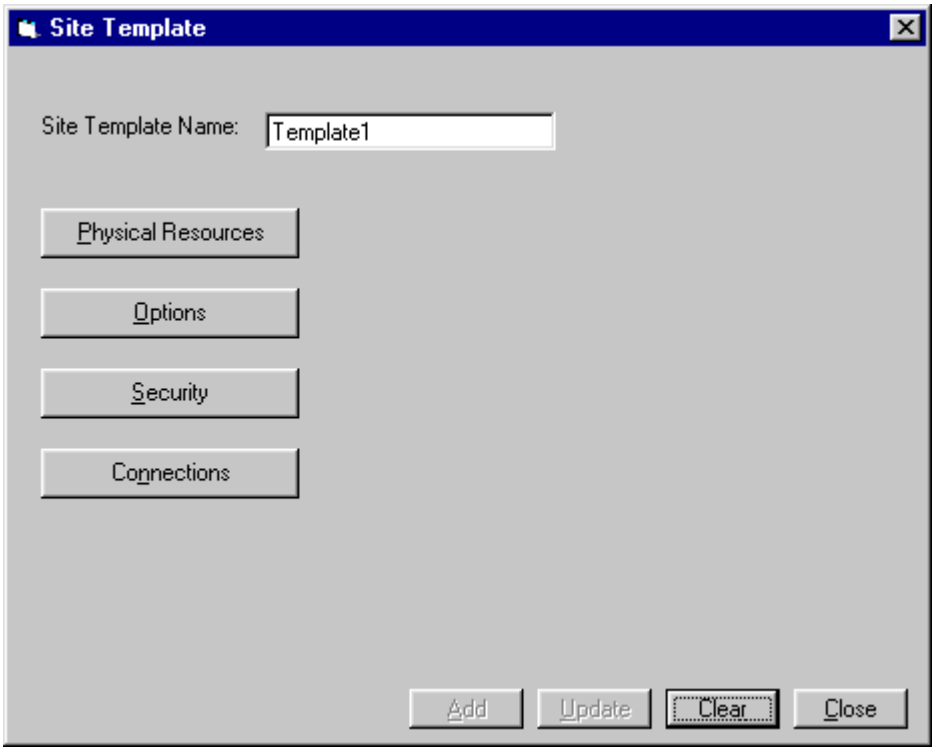
The initial steps to configuring a site template are as follows:

1. From the menu bar, click on *Functions* then again on *Site Templates*, or click on the toolbar. The following screen will be displayed:



2. Click on *Add*.
3. Enter a user-defined template name.
4. Click on *Add*.

5. All *Site Template* configuration options will now be available as shown below:



Note: If you need more than one site template, and the majority of the configuration values will be the same, the *Duplicate* option included on the initial site template window is a valuable tool. To use the *Duplicate* option:

- On the initial site template window, click once on the name of the previously configured template you want to duplicate.
- Click on the *Duplicate* button.
- Enter the name for the new *Site Template*.
- Double click on the new site template's name (it was added to the selection possibilities after the last step).
- Make the necessary changes to the template.

CONFIGURING TEMPLATE PHYSICAL RESOURCES

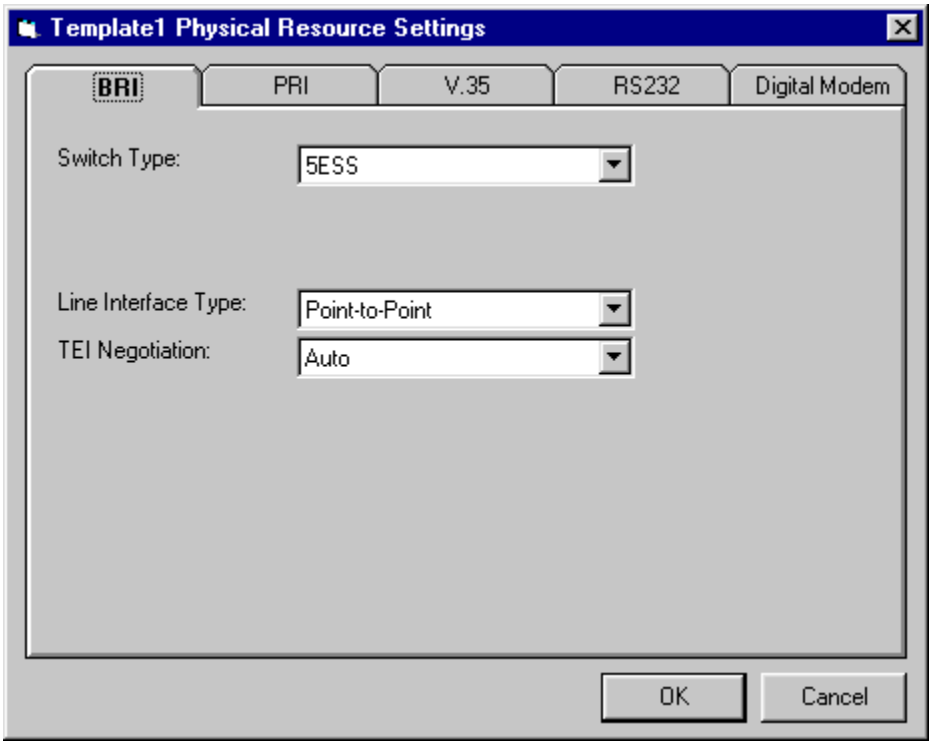
Physical resource are physical interfaces for the attachment of lines (i.e., connections) to a system. Supported physical resources include:

- Basic Rate (BRI)
- Primary Rate (PRI)
- V.35
- RS232
- Digital Modem

To begin configuring your template's physical resources, click on *Physical Resources* from the *Site Template* dialog box. Use the resulting dialog box and the following sections to configure each type of resource.

CONFIGURING BASIC RATE (BRI) RESOURCES

This section shows you how to configure BRI resources for the site template. The screen below shows a basic BRI configuration.



1. Select a *Switch Type.*

2. If you select the *NET3* switch type, select a *Switch Country*. The switch country associates the switch type with the particular European country in which the site is located.

3. If you select the *Teleos Simulator* switch type you will need to select its *Simulated Switch Type.*

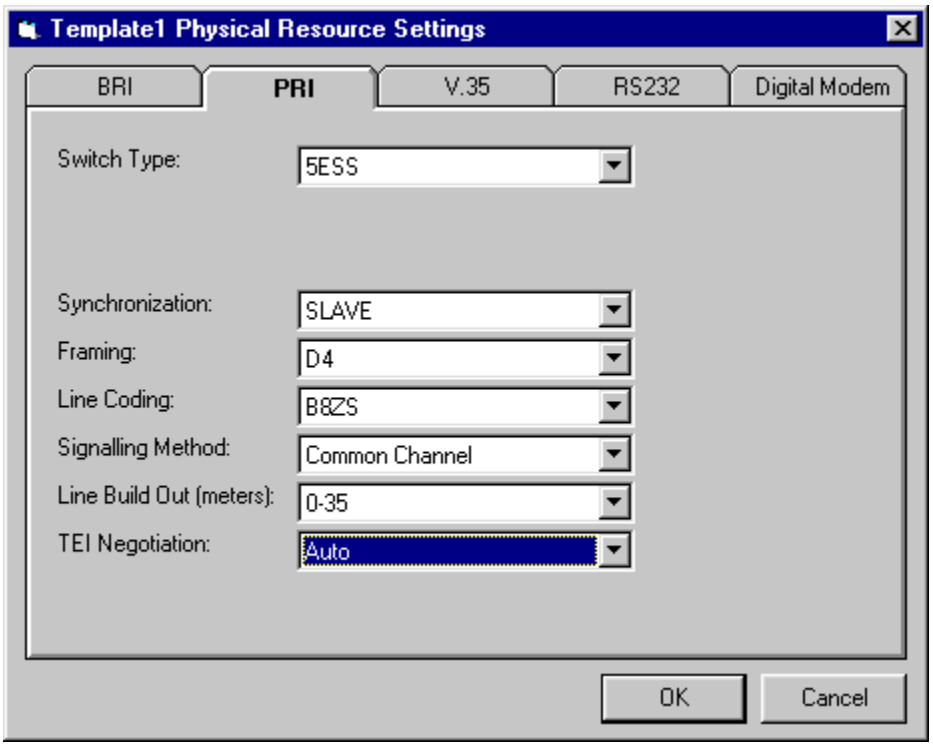
4. Select a *Line Interface Type*. The point-to-point interface type is most often used in the US; point-multipoint is most often used in Japan.

5. Select a *TEI Negotiation* scheme. This designates whether or not Automatic TEI Negotiation will be used. Select Automatic TEI Negotiation (*Auto*) UNLESS the network contains point-to-point NTT lines.

6. If you select *Non-Auto* for the *TEI Negotiation scheme,* you will need to enter a TEI value. A TEI value of 0 is normally correct for a point-to-point NTT line.

CONFIGURING PRIMARY RATE (PRI) RESOURCES

This section shows you how to configure PRI resources for the site template. The screen below shows a basic PRI configuration.



1. Select a *Switch Type.*

2. If you select the *NET5* switch type, select a *Switch Country*. The switch country associates the switch type with the particular European country in which the site is located.

3. If you select the *Teleos Simulator* switch type you will need to select its *Simulated Switch Type.*

4. Select a *Synchronization* type. Every framed transmission line requires a clock source from which it must derive the appropriate bit timing and channel timing relative to the start of a frame. For most CPE gear, the clocking is derived from the received signal and the transmission clock is thus a *slave* to the network. However, if the line is to provide its own clocking, it must

derive a clock from an internal source rather than a received signal. The line is then a *master* clock source.

5. Select a *Framing* type. The two most common framing types for PRI/T1 lines are DF and ESF, which are 12- and 24-frame formats, respectively. E1 lines can use one of three framing types: doubleframe, multiframe with no CRC, or multiframe with CRC, with the most common being multiframe CRC.

6. Select a *Line Coding* type. Line coding specifies the nature of the signals that are used to represent binary one and zero at the physical layer. Choices are Alternate Mark Inversion (*AMI*) and Bipolar 8 Zero Substitution (*B8ZS*).

7. Select a *Signaling Method*. The signaling method dictates how and where the call signaling is to be carried. With *Common Channel* signaling, one of the 24 channels of the PRI frame is devoted to call control messaging. With *Robbed Bit* method, 1 bit of each data channel is "robbed" in order to carry the requisite signaling information.

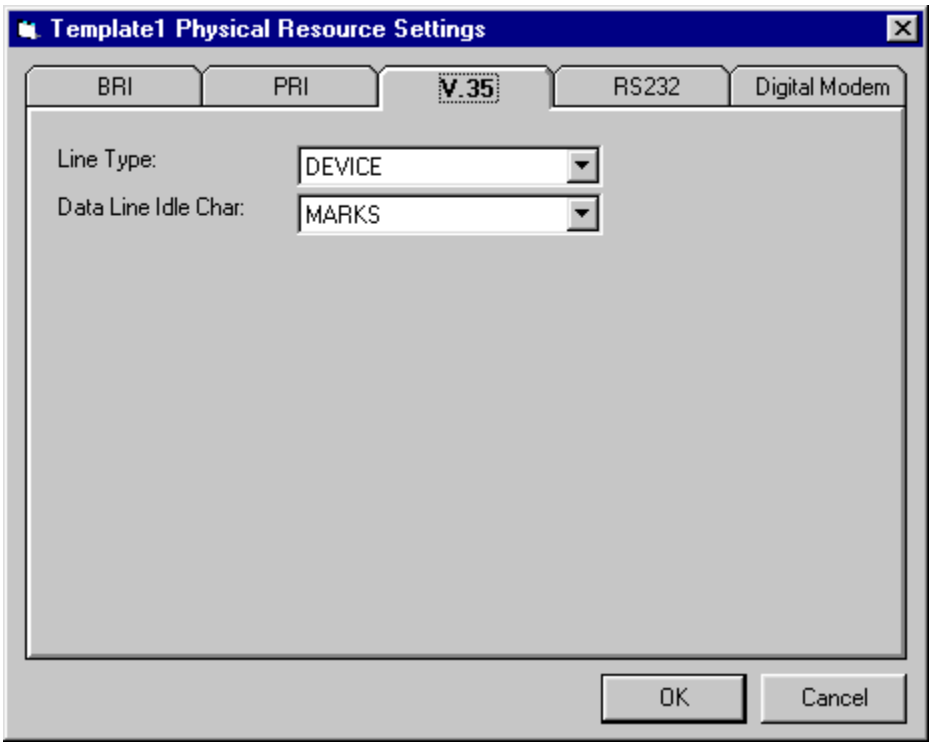
8. Select a *Line Build Out* value (in meters). No matter what the quality of the cabling employed in a network, every line experiences some signal loss or degradation. The line build out describes the degree of attenuation to be applied to the transmission signal in order to have the correct signal levels and shape arrive at the receiver. Generally, the longer the line connecting the CPE and the network equipment, the lower the line build out parameter, and therefore the less the transmitted signal is attenuated.

9. Select a *TEI Negotiation* scheme. This designates whether or not Automatic TEI Negotiation will be used. Select Automatic TEI Negotiation (*Auto*) UNLESS this is a point-to-point NTT line.

10. If you select *Non-Auto* for the *TEI Negotiation scheme*, enter a TEI value. A TEI value of 0 is normally correct for a point-to-point NTT line.

CONFIGURING V.35 OR RS232 RESOURCES

This section shows you how to configure V.35 and RS232 resources for the site template. The parameters are identical for both resources. The screen below shows a basic V.35 configuration.

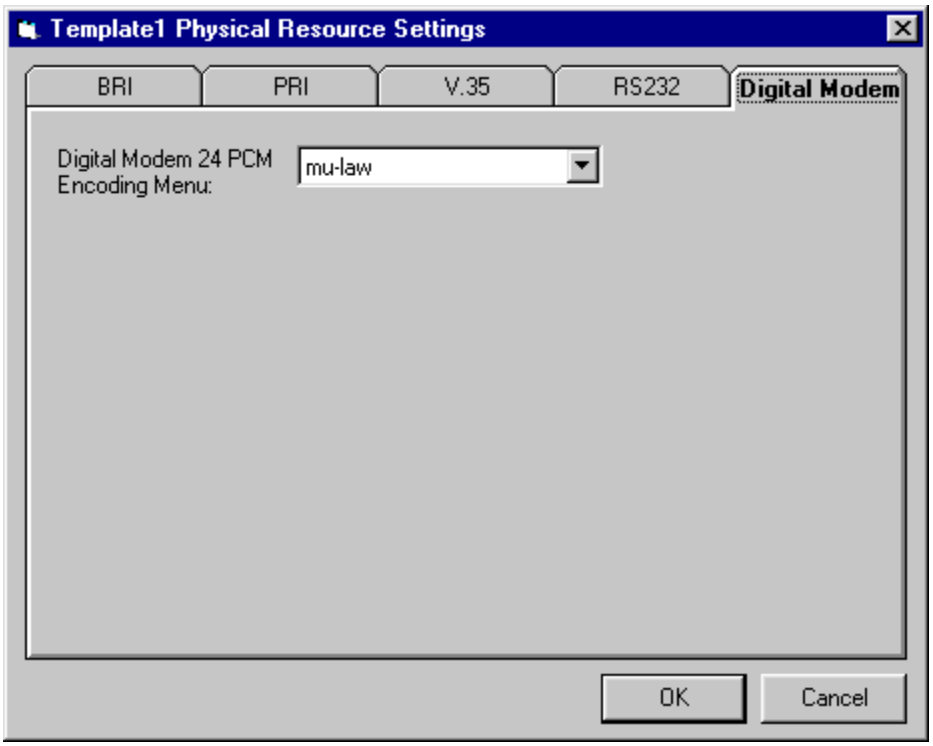


1. Select a *Line Type*. This differentiates the network connections from local computing device connections. The *network* line type is specified for lines using a dedicated, frame relay, or X.25 access.

2. Select a *Data Line Idle Character*. This identifies the idle character which is transmitted by the Cabletron system between the HDLC frames. The character choices are *marks* (all '1's) or HDLC *flags* (hexadecimal '7E'), with marks being the default. In most situations, the default value is acceptable, as the receiving side should be able to identify the start of a new frame after reception of either idle character. However, there may be some receiving devices that cannot make this determination with the default of idle marks. If communication cannot be established with the receiving device, you may need to set the idle character to a value that the receiving device will understand.

CONFIGURING DIGITAL MODEM RESOURCES

This section shows you how to configure a digital modem resource for the site template. The configuration information applies only to the DM-24 resource (24 port digital modem card). The screen below shows a basic digital modem configuration.



The only configurable field for the DM-24 is the *PCM Encoding Menu*. This is the Pulse Code Modulation (PCM) encoding method appropriate for your country. Choices include mu-law and A-law.

CONFIGURING TEMPLATE OPTIONS

Site options allow you to configure site template information for the following categories:

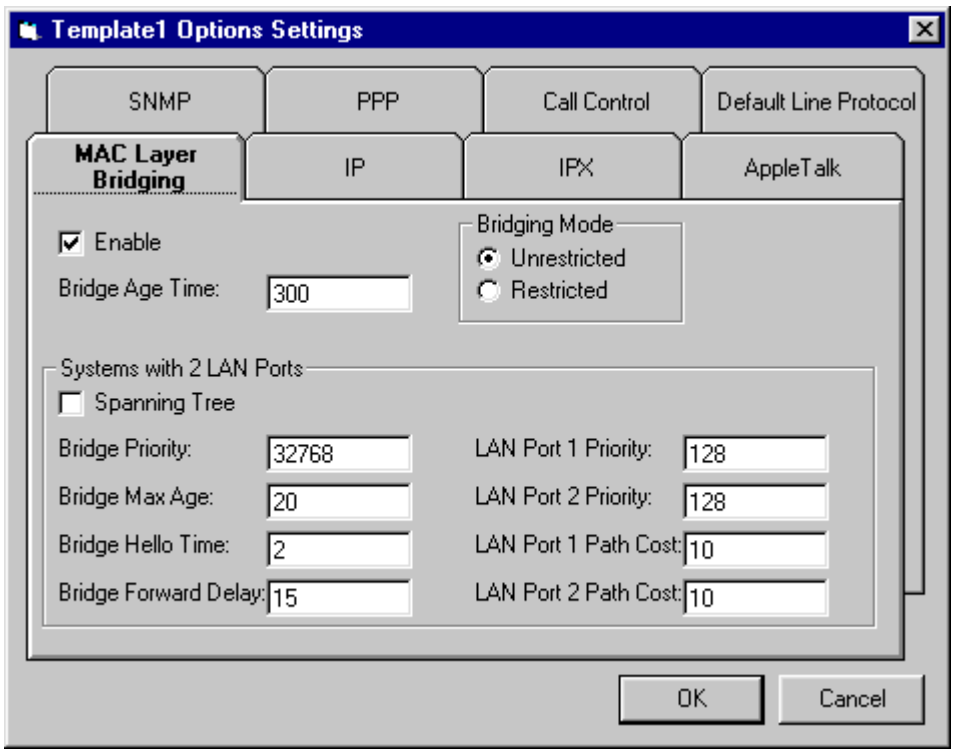
- MAC Layer Bridging
- IP
- IPX
- AppleTalk
- SNMP
- PPP
- Call Control
- Default Line Protocol

To begin configuring your template's options, click on *Options* from the *Site Template* dialog box. Use the resulting dialog box and the following sections to configure each site template option.

CONFIGURING MAC LAYER BRIDGING INFORMATION

This section shows you how to configure MAC layer bridging information for the site template. The screen below shows a basic MAC layer bridging configuration.

Note: The default values are suitable for most configurations.



1. For sites using MAC layer bridging, make sure *Enable* is checked as shown above. All other bridging parameters will then take effect.

2. Enter the *Bridge Age Time* (in seconds). This is the amount of time a bridge will keep a MAC address it learns before that address expires. The default value is 300 seconds. This parameter is available for systems with 1 or 2 LAN ports.

3. Select the *Bridging Mode*. This allows you to determine the forwarding method that the bridge uses to distribute LAN packets to the remote sites and to the LAN ports of the system. Possible modes of operation are *Unrestricted* and *Restricted*. The default is unrestricted. In general, the unrestricted mode forwards all packets, whereas the restricted mode discards all packets.

4. If you have a system with 2 LAN ports, you can make use of all Spanning Tree Protocol parameters. First, enable *Spanning Tree* (click on *Spanning Tree* and a check will appear in the box adjacent to it). Next, define the Spanning Tree parameters.

   a. *Bridge Priority*: The configured priority for this system.

   b. *Bridge Max Age*: The configured maximum age-time (in seconds) for this system when the system is the root bridge.

c. *Bridge Hello Time*: The configured hello time interval (in seconds) for this system when the system is the root bridge.

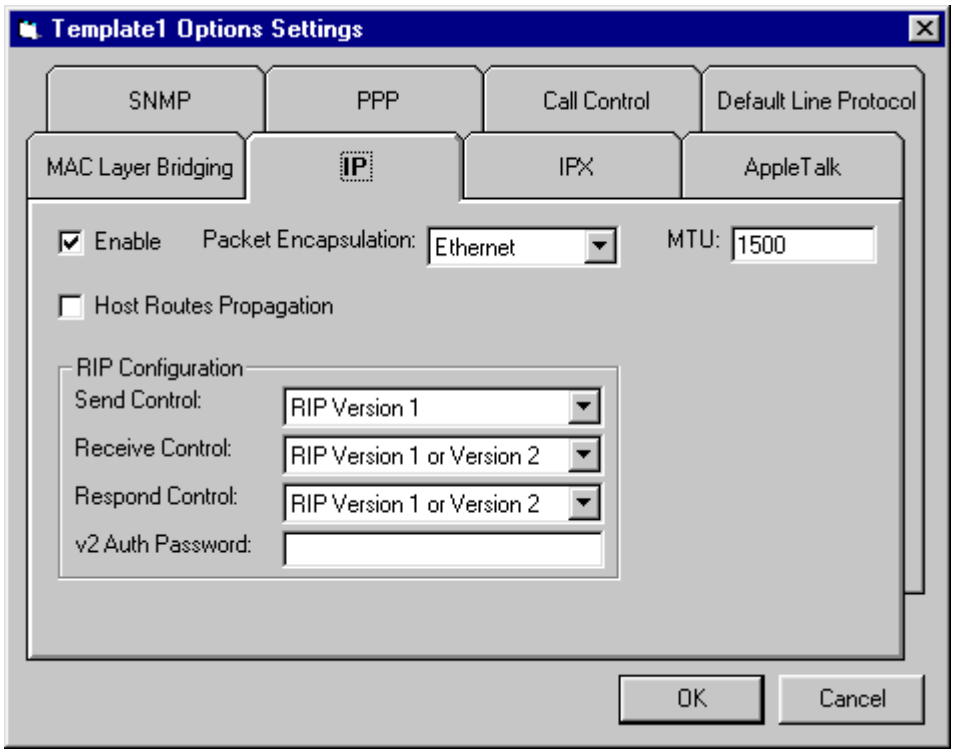
d. *Bridge Forward Delay*: The configured forward delay time (in seconds) for this system when the system is the root bridge.

e. *LAN Port <1 or 2> Priority*: The configured priority for the indicated port.

f. *LAN Port <1 or 2> Path Cost*: The configured path cost for the indicated port.

CONFIGURING IP INFORMATION

This section shows you how to configure IP information for the site template. The screen below shows a basic IP configuration.



1. For sites using IP routing, make sure *Enable* is checked as shown above.

2. Select a *Packet Encapsulation* type. This is the encapsulation type for IP datagrams transferred on this interface. *Ethernet* type encapsulation specifies that IP datagrams are transferred in standard Ethernet frames as specified in RFC-894. *SNAP* type encapsulation specifies that IP datagrams are transferred in 802.3 format frames using the Sub Network Access Protocol (SNAP) as specified in RFC-1042.

3. Enter an *MTU* value. This is the maximum number of bytes that can be transmitted on the network interface. Some devices on the network may not be able to receive large data packets.

This parameter allows you to maintain compatibility with these devices by setting the MTU to agree with that supported by the device.

4. Select a *Host Routes Propagation* scheme. This controls how the IP RIP packets are propagated. If disabled, WAN local routes are propagated as subnetwork routes. If enabled, host routes will be propagated on other network interfaces only while each remote IP device is connected to the site.

   Also, when enabled, it will allow multiple systems on the same LAN to work properly. IP RIP information is then advertised as multiple host routes as they connect to the site.

5. Enter the *RIP Configuration*.

   a. *Send Control*: Controls how IP RIP update messages are sent on an IP RIP interface. The following table provides possible choices for IP RIP send control.

Choice	*Meaning*
Do Not Send	This switch indicates sending no IP RIP packets at all.
RIP Version 1	This switch indicates sending IP RIP updates compliant with RFC 1058.
RIP Version 1 Compatibility	This switch indicates broadcasting IP RIP v2 updates using RFC 1058 route subsumption rules.
RIP Version 2	This switch indicates multicasting IP RIP v2 updates compliant with RFC 1723.

   b. *Receive Control*: Controls which version of IP RIP updates are to be accepted. The following table provides possible choices for IP RIP receive control.

Switch	*Meaning*
Do Not Receive	This switch indicates accepting no IP RIP updates at all.
RIP Version 1 Only	This switch indicates accepting only IP RIP updates compliant with RFC 1058.
RIP Version 2 Only	This switch indicates accepting only IP RIP v2 updates compliant with RFC 1723.
RIP Version 1 or Version 2	This switch indicates accepting either IP RIP v1 or IP RIP v2 updates.

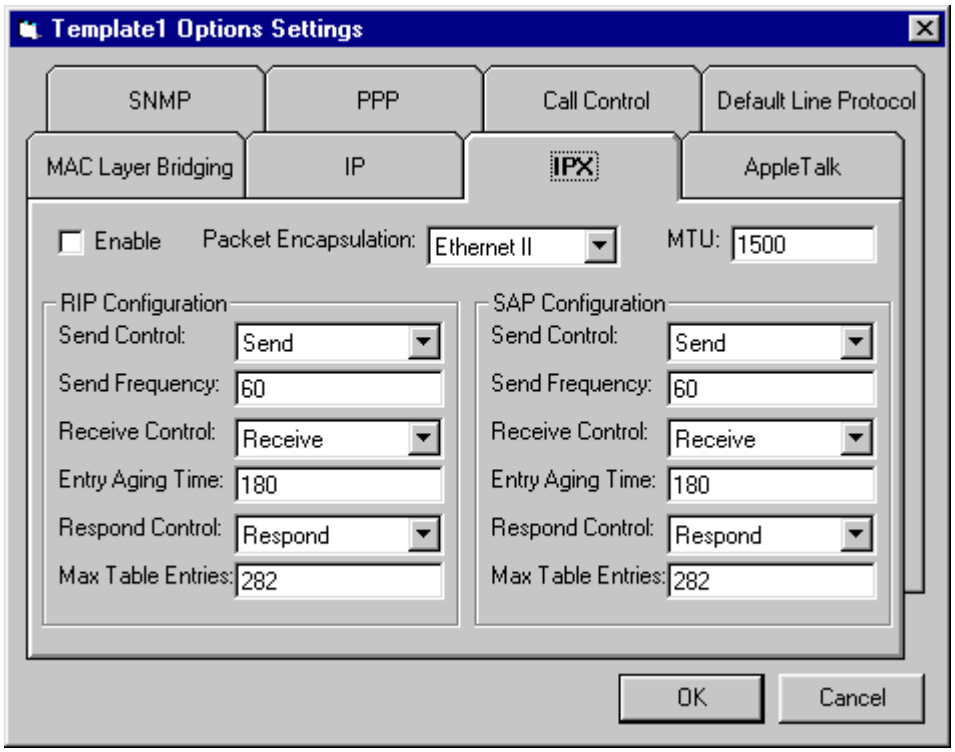
   c. *Respond Control*: Controls how the system responds to IP RIP requests on the interface. The following table provides possible choices for IP RIP respond control.

Switch	*Meaning*
Do Not Respond	This switch indicates responding to no IP RIP requests at all.
RIP Version 1 Only	This switch indicates responding only to IP RIP requests compliant with RFC 1058.
RIP Version 2 Only	This switch indicates responding only to IP RIP v2 requests compliant with RFC 1723.
RIP Version 1 or Version 2	This switch indicates responding with the same IP RIP version format as the version of the request.

d. *v2 Auth Password*: This password is only required if the site will be using IP RIP v2 with a password required. The password is user-defined, 1-16 characters in length.

CONFIGURING IPX INFORMATION

This section shows you how to configure IPX information for the site template. The screen below shows a basic IPX configuration.



1. For sites using IPX, make sure *Enable* is checked. When enabled, the system will process and forward IPX data packets at the IPX network layer. When disabled, the system will process and forward IPX data packets at the MAC or bridging layer.

2. Select a *Packet Encapsulation* type. This specifies the IPX datagram encapsulation type in use. NetWare supports four types of encapsulation: Novell ETHERNET_SNAP, Novell Ethernet

802.3, Novell ETHERNET_II, and Novell Ethernet 802.2. The Ethernet 802.3 type is the default type for NetWare v2.x and v3.x. The Ethernet 802.2 type is the default type for NetWare v4.x.

3. Enter an *MTU* value. This specifies the maximum number of bytes that can be transmitted on the network interface. Some devices on the network may not be able to receive large data packets. This parameter allows you to maintain compatibility with these devices by setting the MTU to agree with that supported by the device.

4. Enter the *RIP/SAP Configuration* information.

    a. *Send Control*: Specifies how the site will send RIP / SAP information. When set to *Send*, the site will transmit IPX RIP / SAP packets. When set to *Do Not Send*, the site will not transmit any IPX RIP / SAP packets.

    b. *Send Frequency*: Specifies the frequency (in seconds) at which the systems at the site will transmit RIP / SAP packets (when the Send control parameter is set to *Send).*

    c. *Receive Control*: Specifies how the site will process RIP / SAP packets received. When set to *Receive*, the site will process IPX RIP / SAP packets received and will update its internal routing tables. When set to *Do Not Receive*, the site will not process any IPX RIP / SAP packets.

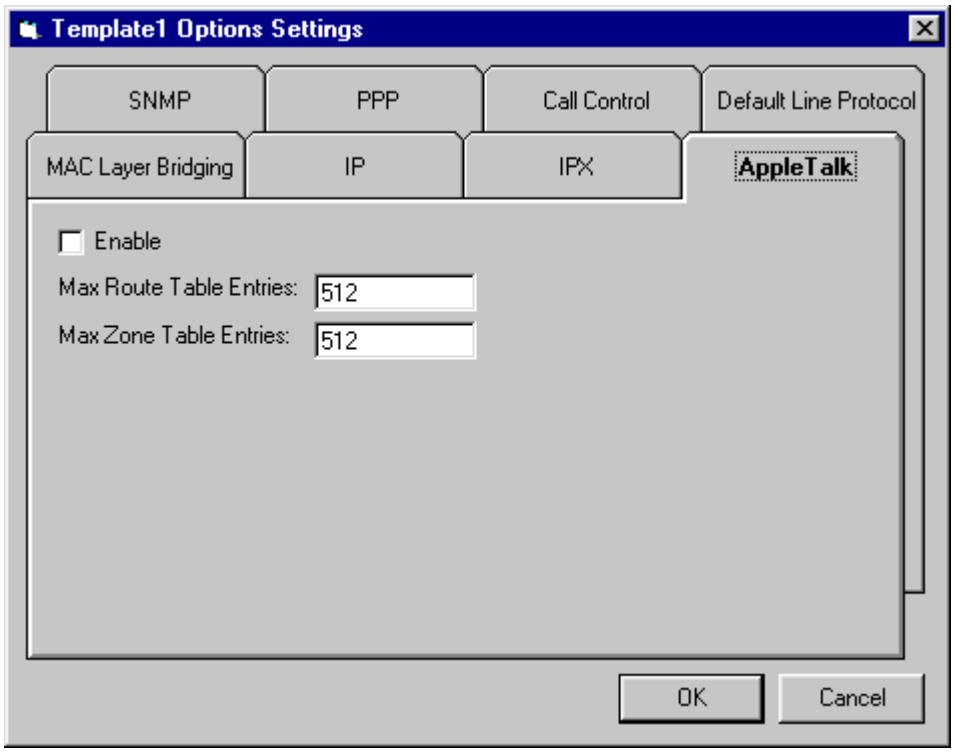
    d. *Entry Aging Time*: Specifies the time (in seconds) it takes for the systems at the site to age out and make a learned dynamic Routing table entry inactive.

    e. *Respond Control*: Specifies how the site should respond to RIP / SAP queries from other devices. When set to *Respond*, the site will transmit a RIP / SAP response to the requesting device. When set to *Do Not Respond*, the site will ignore RIP / SAP Requests received.

    f. *Max Table Entries*: Specifies the maximum number of routing entries which can be stored in the route or service table.

CONFIGURING APPLETALK INFORMATION

This section shows you how to configure AppleTalk information for the site template. The screen below shows the default AppleTalk configuration.



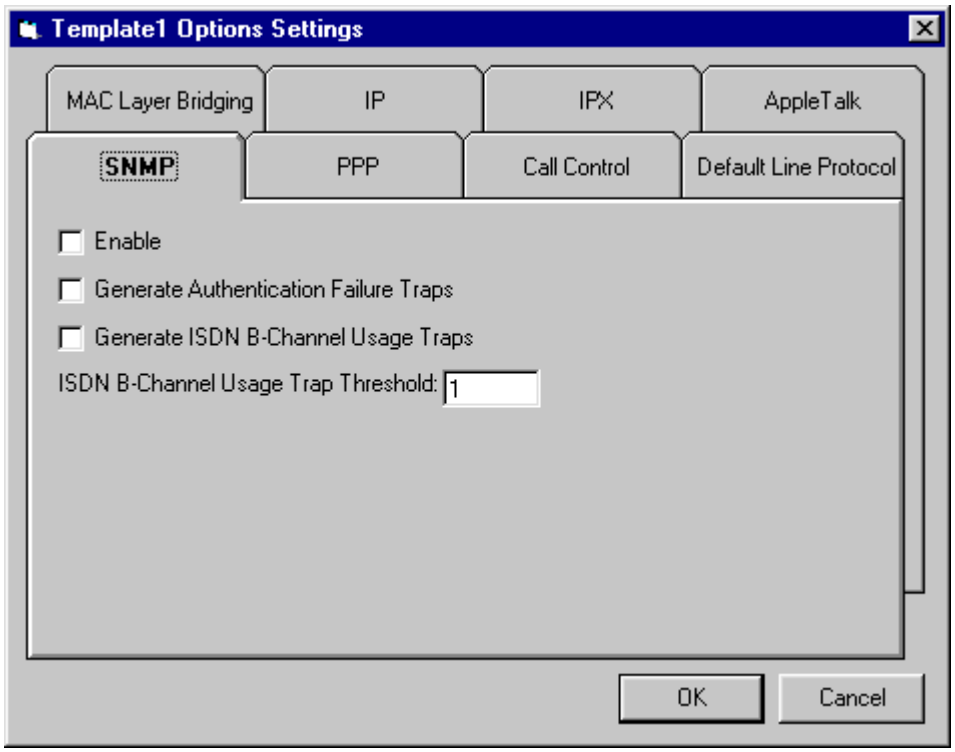
1. For sites using AppleTalk, make sure *Enable* is checked.

2. Enter a value for the *Max Route Table Entries*. This is the maximum number of defined and learned routing table entries.

3. Enter a value for the *Max Zone Table Entries*. This is the maximum number of defined and learned zone table entries.

CONFIGURING SNMP INFORMATION

This section shows you how to configure SNMP information for the site template. The screen below shows a basic SNMP configuration.



1. For sites using SNMP, make sure *Enable* is checked. All SNMP parameters will then take effect. On the above screen, SNMP is disabled.

2. Select whether or not the site's systems will *Generate Authentication Traps*. The snmpEnableAuthenTraps object of the MIB-II SNMP group will be initialized to what you configure (either enabled or disabled).

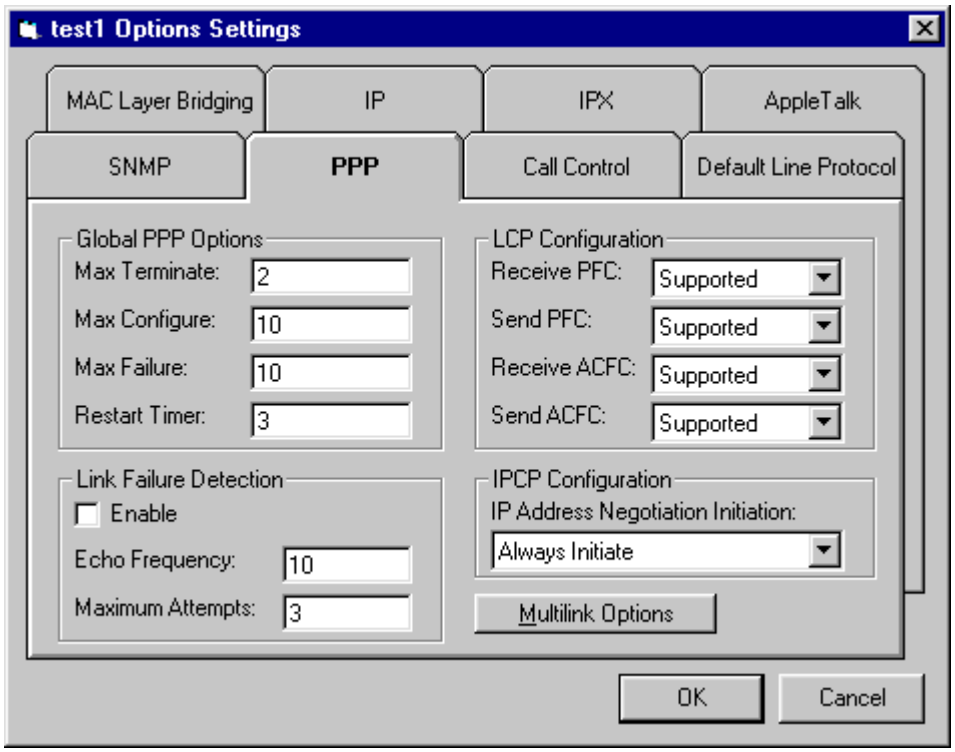
3. Select whether or not the site's systems will *Generate ISDN B-Channel Usage Traps*. When enabled, you can use these generated traps to monitor the system's ISDN B-channel usage. There are two distinct ISDN B-Channel Usage Traps. The isdnUsageHigh trap is generated when the B-channel threshold (configured below) is met or exceeded. The isdnUsageNormal trap is generated when the number of B-channels in use drops back below the configured threshold value.

4. Set the *ISDN B-Channel Usage Trap Threshold*. This value is used to trigger the ISDN B-Channel Usage Traps. The threshold value is a number between 1 and the total number of available B-channels.

CONFIGURING PPP INFORMATION

This section shows you how to configure PPP information for the site template. The screen below shows a basic PPP configuration.

Note: A thorough understanding of PPP protocol is required before you attempt to change the PPP configuration. By changing the PPP configuration, you are changing the PPP protocol negotiation parameters. These parameters only need to be changed when you are interoperating with devices that do not provide a standard PPP implementation. Changing these parameters can result in PPP option negotiation failure and the inability to communicate with remote devices. The default parameters are adequate for most sites.



1. Enter the *Global PPP Options* values.

   a. Enter the *Max Terminate*. This is the number of Terminate-Request packets sent without receiving a Terminate-Ack before assuming that the peer is unable to respond.

   b. Enter the *Max Configure*. This is the number of Configure-Request packets sent without receiving a valid Configure-Ack, Configure-Nak, or Configure-Reject before assuming that the peer is unable to respond.

   c. Enter the *Max Failure*. This is the number of Configure-Nak packets sent without sending a Configure-Ack before assuming that configuration is not converging. Any additional Configure-Nak packets are converted to Configure-Reject packets.

   d. Enter the *Restart Timer* value. This times transmissions of Configure-Request and Terminate-Request packets. Expiration of the timer causes a timeout event, and retransmission of the corresponding Configure-Request or Terminate-Request packet.

2. Select the *LCP Configuration* values.

   a. Select the *Receive PCF/ACFC* values. These control whether (and how) the site's systems receive PPP packets with PFC or ACFC. Receive setting options include:
      - mandatory (requested, repeated indefinitely if NAK'd)
      - preferable (requested, repeated up to Max Attempt times if NAK'd)
      - supported (not requested, a peer request will be ACK'd)
      - not supported (not requested, NAK'd if the peer requests it)

   b. Select the *Send PCF/ACFC* values. These control whether (and how) the site's systems send PPP packets with PFC or ACFC. Send setting options include:
      - mandatory (requested, repeated indefinitely if NAK'd)
      - preferable (requested, repeated up to Max Attempt times if NAK'd)
      - supported (not requested, a peer requst will be ACK'd)
      - not supported (not requested, NAK'd if the peer requests it)

3. Configure the *Link Failure Detection* option.

   a. If you *enable* this option, there will be a periodic transmission of Echo-Request frames (a maintenance type frame provided by PPP's Link Control Protocol). Reception of the appropriate Echo-Reply frame indicates a properly functioning connection; incorrect replies or lack of replies indicate a connection failure.

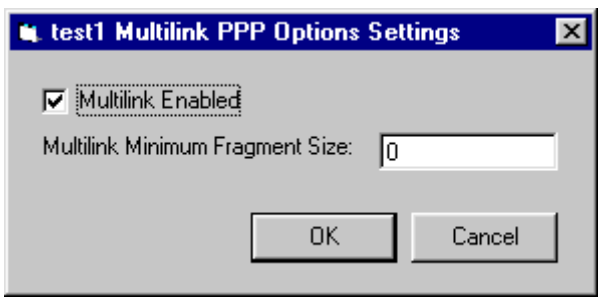
   b. Enter the *Echo Frequency*. This specifies, in seconds, how often the Echo-Request frames are transmitted.

   c. Enter the *Maximum Attempts*. This specifies how many consecutive Echo-Requests are sent without receiving a reply before declaring the PPP link to be faulty.

4. Complete the *IPCP Configuration*.

   Select the *IP Address Negotiation Initiation* value. This defines when IPCP will initiate IP address IPCP option negotiation. Possible choices are:
   - *Always Initiate* (IPCP will always initiate the IP address option negotiation on a PPP link)
   - *Initiate if IP Address Unknown* (IPCP will initiate the negotiation only when the peer's IP address is unknown)

5. Configure the *Multilink Options*. Note that you should not have to change the default configuration for multilink options. The example below shows the default configuration.



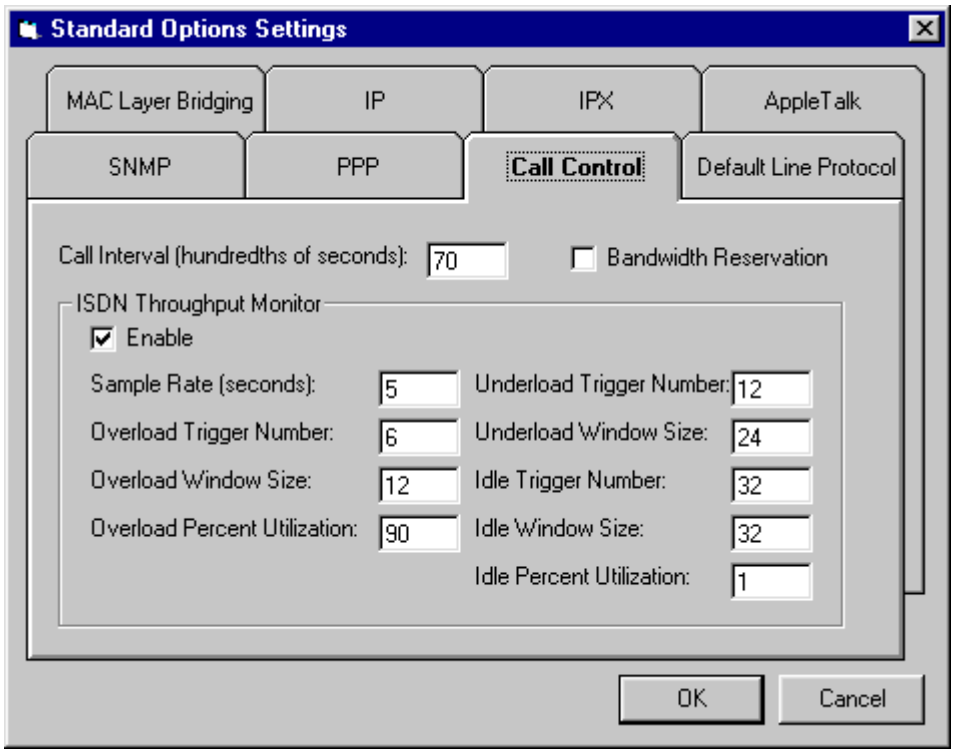
a. You may enable or disable Multilink support. Once you have enabled Multilink, the following Multilink parameter will take effect.

b. Enter the *Multilink Minimum Fragment Size*. When transmitting data over multiple channels, the normal algorithm is to divide the original packet into proportional fragments for transmission over all the channels in the group. This option dictates a minimum size for the fragments, with the intent being to avoid the transmission of very small fragments. The parameter is actually expressed as fragment transmission time, in units of .1 milliseconds. For example, a minimum fragment size of 64 bytes on a 64,000 Kbits / second link would be expressed as 80 (64bytes / (8000bytes / sec) = 8 msec ==> 80).

Note: The reduced processing burden due to avoidance of small fragments comes at the potential expense of wasted bandwidth, since some channels may be left idle when transmitting a packet.

CONFIGURING CALL CONTROL INFORMATION

This section shows you how to configure call control information for the site template. The screen below shows the default call control configuration.



1. Enter the *Call Interval* value (in hundredths of seconds). This is the minimum time between call attempts. The site's systems will not make a call attempt in less than the configured call interval value. However, due to the system clock resolution, the actual time interval may be greater than the configured value. The default value is .70 seconds. The range of the configured value is 0 to 5 seconds, in 1 / 100 second increments. A configured value of 0 implies that the system will make call attempts without any delay between attempts.

2. You may enable (with a check) or disable (no check, as shown above) *Bandwidth Reservation* for the template. The bandwidth reservation feature allows a portion of possible system connections to always be available to specific users for both inbound and outbound calls. For a more detailed description of the Bandwidth Reservation feature, refer to *Circuit Groups Information* (in the *Configuring Sites* chapter).

3. Complete the *ISDN Throughput Monitor* configuration.

   When *enabled*, this feature samples the amount of data transmitted and received on the connections between two systems. Each sample compares data associated with overload, underload, and idle conditions. A history of these comparisons is kept in a sliding window. The window size, number of samples needed to trigger an event, and sampling frequency are configurable.

   The default throughput monitor configuration delivered with the system will work for initial system installation. Later, these parameters can be changed to better match the bandwidth needs of the site location.

   a. Set the *Sample Rate (seconds)*. This is the number of seconds for each sample period. During this time period, the system keeps track of total number of bytes transmitted to and received from another system. The utilization percentage is determined by comparing this total with the realistic maximum for the current aggregate amount of bandwidth.

   b. Set the *Overload Trigger Number*. This is the number of samples within the window that must exceed the specified utilization for the overload condition to occur.

   c. Set the *Overload Window Size*. This is the number of sample periods (up to 32) that will be used for the sliding overload window.

   d. Set the *Overload Percentage Utilization*. This is the percentage of available bandwidth that the traffic samples must exceed for an overload condition to occur.

   e. Set the *Underload Trigger Number*. This is the number of samples within the window that must be below the next lowest target capacity for the underload condition to occur.

   f. Set the *Underload Window Size*. This is the number of sample periods (up to 32) that will be used for the sliding underload window.

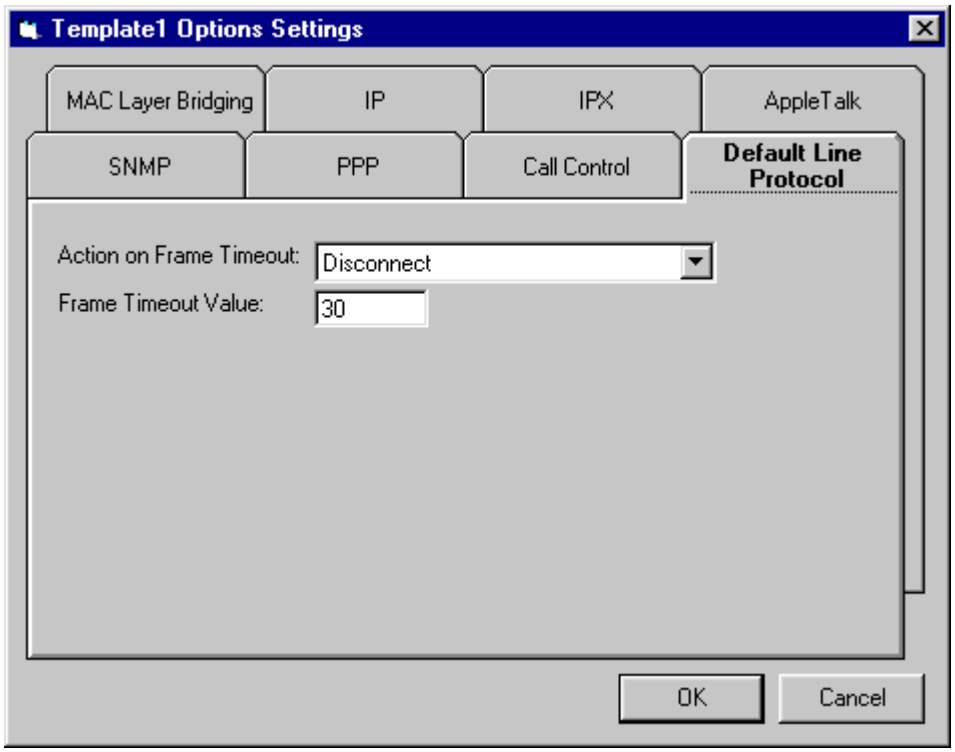
   g. Set the *Idle Trigger Number*. This is the number of samples within the window that must be below the specified utilization for the idle condition to occur.

   h. Set the *Idle Window Size*. This is the number of sample periods (up to 32) that will be used for the sliding idle window.

   i. Set the *Idle Percent Utilization*. This is the percentage of available bandwidth on the last connection that traffic samples must fall below for the connection to be considered idle.

CONFIGURING DEFAULT LINE PROTOCOL INFORMATION

This section shows you how to configure default line protocol information for the site template. The screen below shows the initial default line protocol configuration.



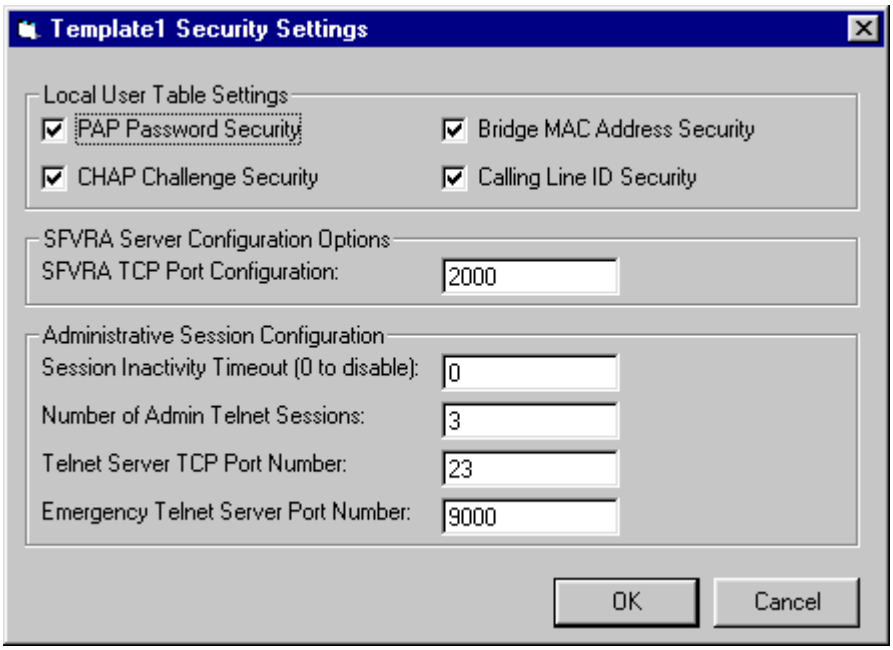
When a connection occurs, the system waits for a packet to arrive, and from that packet, it determines the protocol type being used. After a default frame timeout value of 30 seconds, if no packet is received, the default action on frame timeout is to disconnect the call. Through the Default Line Protocol dialog box (as shown above), you may change the default action and default timeout value.

1. Select the *Action on Frame Timeout*. This is the action to be taken if no frame is received before the configured frame timeout value has expired. Possible actions are:
   - Disconnect
   - Use HDLC Bridge Protocol
   - Use IP Host Protocol (RFC 1294)
   - Use PPP Protocol

2. Enter the *Frame Timeout Value*. This is the time limit (in seconds) to wait to receive a packet.

CONFIGURING TEMPLATE SECURITY INFORMATION

This section shows you how to configure security information for the site template. The security information will apply to each system added to the site using this template. The screen below shows the default security configuration.



1. For sites using a local user table for authentication, you will need to complete *Local User Table Settings*. Enable each security option that the site's systems will use to authenticate remote users. In the above example screen, all four local user table security options are enabled. (A check mark indicates that the option is enabled.)

2. For sites using an SFVRA database for authentication, you will need to complete the *SFVRA Server Configuration Options*. Currently, the only entry you will need to complete is the *SFVRA TCP Port Configuration*. This is the port number used by the SFVRA Connection Manager. Note that you can assign a user-defined port number, but that the SFVRA's TCP port number must be entered identically here and on the SFVRA Connection Manager.

3. Enter the *Administrative Session Configuration* values.

    a. Enter the *Session Inactivity Timeout*. This parameter allows you to terminate login sessions after the configured length of time (the timeout value). The default value is 0, which disables the timeout feature. When disabled, login sessions will not be timed out. To enable the feature, enter a value greater than 0.

    b. Enter the *Number of Admin Telnet Sessions*. This parameter disables, or limits the number of Telnet administrative sessions allowed. If 0 is entered, the Telnet server will be disabled.

    c. Enter the *Telnet Server TCP Port Number*. The port number of the Telnet server TCP port.

    d. Enter the *Emergency Telnet Server Port Number*. The port number for emergency Telnet sessions.When you need Telnet access to a system, but all available Telnet sessions are in

use, you may use the emergency Telnet server to clean up "dead" Telnet sessions. This Telnet server needs a unique port number.

CONFIGURING TEMPLATE CONNECTIONS INFORMATION

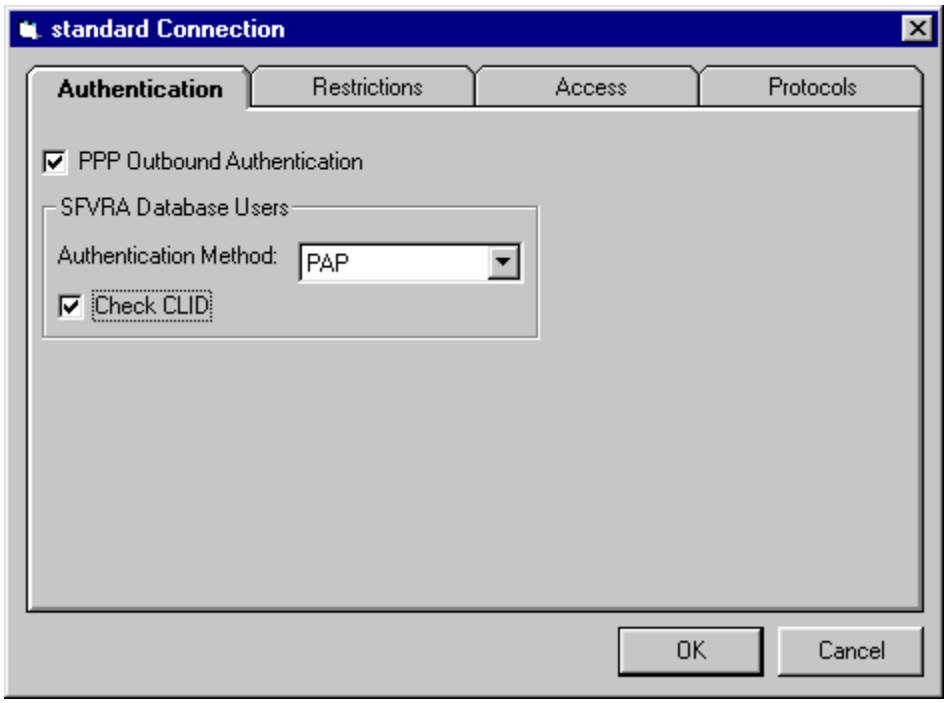
This section shows you how to configure connections information for the site template. Connections information dictates how the site's systems will handle connections. Later, when connection groups are configured (refer to *Configuring Connection Groups*), the SFVRA-CFG incorporates site template connection information into the connection group configuration.

Connection information is divided into the following categories:

- Authentication
- Restrictions
- Access
- Protocols

CONFIGURING AUTHENTICATION INFORMATION

Authentication information is divided into two sections: authentication information for systems doing authentication through (a) local user tables and through (b) SFVRA databases.



For systems using local authentication, you may enable or disable *PPP Outbound Authentication*. When PPP outbound authentication is enabled, PPP (CHAP or PAP) authentication is required at both ends of the connection. When PPP outbound authentication is disabled, the remote device that the Cabletron system is calling out to is not required to authenticate itself, but the remote device will authenticate the Cabletron system. In the above example, PPP outbound authentication is enabled.

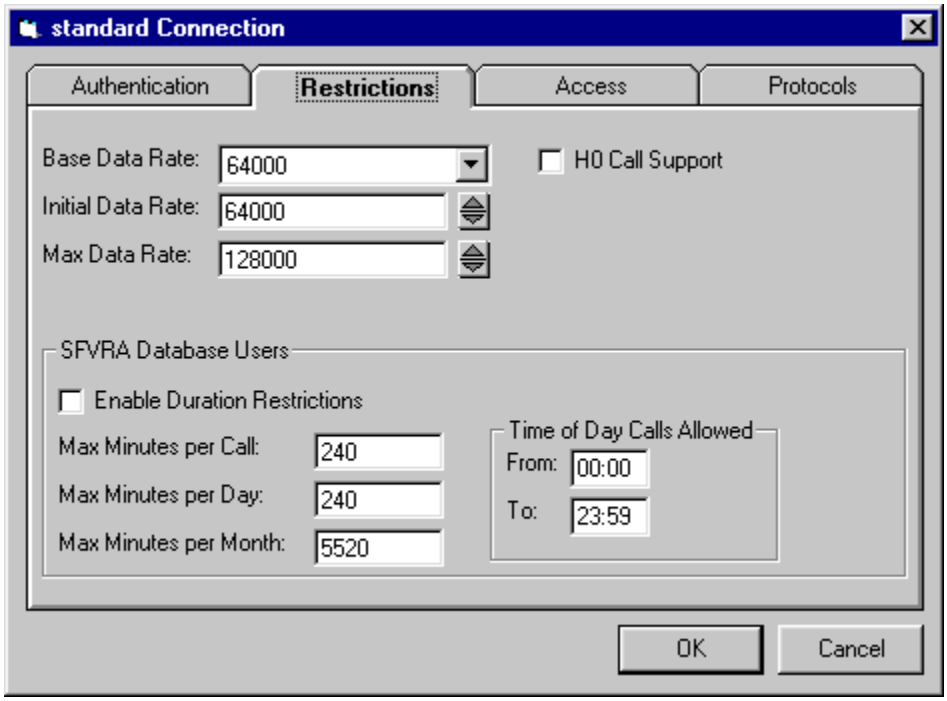
For systems using an SFVRA database for authentication, select an *Authentication Method*. Possible authentication methods are:

- *PAP*
- *CHAP*
- *CLID*
- *None*
- *CPP*
- *NT*

You may select CLID alone by selecting CLID from the displayed list. You may also select CLID in conjunction with another authentication method by selecting one method from the displayed list and then clicking on *Check CLID*.

CONFIGURING RESTRICTION INFORMATION

This section shows you how to configure restrictions connection information for the site template. The screen below shows the default restrictions configuration.



1. Select the *Base Data Rate* (in bps). This is the base data rate at which the system connects to remote devices.

2. Select the *Initial Data Rate* (in bps). Determines the number of calls that will be attempted when opening the first wide area connection. This provides you with a mechanism to request that a group of parallel connections be made to a remote device rather than a single connection, allowing data to begin flowing at greater rates without waiting for the Throughput Monitor to detect an overload condition. Calls will be made until an additional call would exceed the configured value. For example, if you have configured the base data rate at 64,000, and the

initial data rate at 256,000, the system would attempt to initially use four calls (connections) running in parallel (256,000 / 64,000 = 4).

3. Select the *Max Data Rate* (in bps). The max data rate limits the total number of channels that can be committed to a single logical connection. This sets an upper boundary for line and capacity utilization. This upper boundary allows you to keep one remote device from crowding out other users and using an unfair share of available resources. This parameter is enforced on inbound and outbound calls. The system will not accept or make a call when the added bandwidth will exceed the configured maximum. For example, if you have configured the base data rate at 64,000 bps, and the maximum data rate at 512,000 bps, the system would use a maximum of eight calls (connections) running in parallel to open up bandwidth (512,000 / 64,000 = 8). The value need not be a multiple of the base data rate. The default configuration for the maximum data rate is 128,000 bps.

4. You may either enable (with a check) or disable H0 call support.

   H0 calls provide one full 384 Kbps channel through the ISDN network, reducing the overhead associated with aggregating multiple channels. H0 call support is a valuable option for systems that need large bandwidth, for example, systems that transfer large files or do video conferencing. This option is not cost effective for systems that generate a smaller amount of network traffic. Note that not all ISDN carriers provide support for H0 calls.

5. For SFVRA database users: you may enable (with a check) or disable *Duration Restrictions*. Once enabled, values you enter for the following parameters will also apply:

   a. Max Minutes per Call
      The amount of time (in minutes) that a call is allowed to be active.

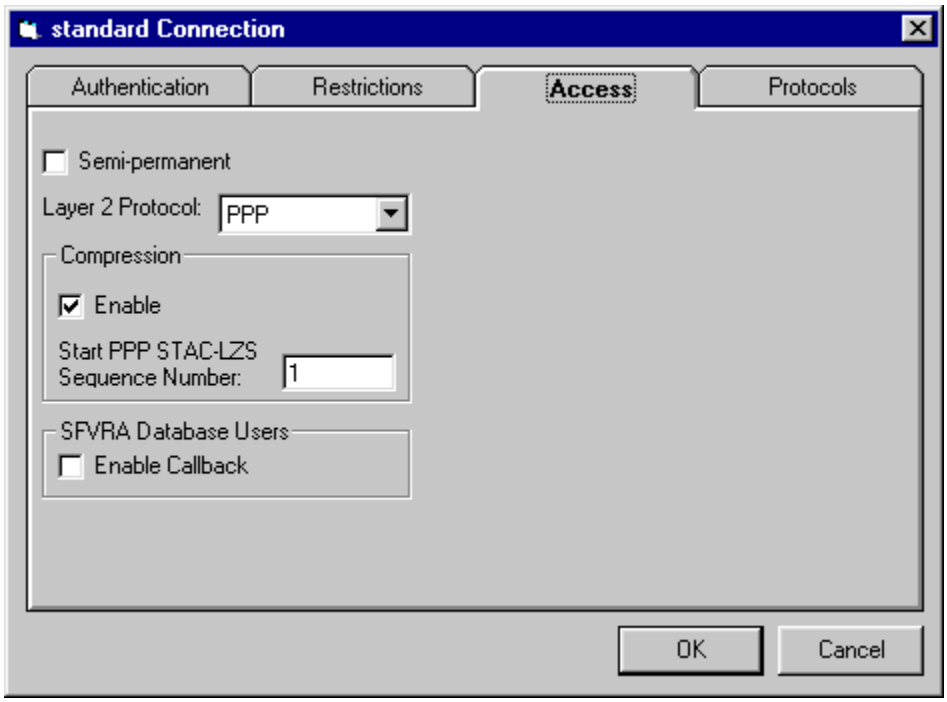
   b. Max Minutes per Day
      The maximum number of call minutes allowed per day.

   c. *Max Minutes per Month*
      The maximum number of call minutes allowed per month.

   d. *Time of Day Calls Allowed*
      The allowable hours for outbound calls (inbound calls will always be allowed).

CONFIGURING ACCESS INFORMATION

This section shows you how to configure access connection information for the site template. The screen below shows the default access configuration.



To edit the default configuration:

1. You may enable or disable the semi-permanent connections option. Click on *Semi-permanent* to enable the semi-permanent option. A semipermanent connection is a connection that is up at all times. One or more switched calls are made at system start-up, and are kept up until system shutdown. This option minimizes the number of calls the system makes, and maximizes the number of active call minutes.

2. Select the *Layer 2 Protocol*. This is the line protocol for ISDN access users. Possible protocols are:
   - *PPP* (Point-to-Point Protocol)
   - *CPP* for Combinet devices (Combinet Proprietary Protocol)

3. Enter *Compression* information.

   a. Check *Enable* to enable the compression option. Once compression is enabled, the following parameter will also apply.

   b. Enter the *Start PPP STAC-LZS Sequence Number*. When using PPP compression with the STAC-LZS protocol, certain devices may not adhere to the protocol specification's requirement that sequence numbers begin with 1, resulting in a resynchronization sequence on the first frame which is exchanged. When the peer fully supports the CCP protocol's Reset mechanism, this will only result in the minor inconvenience of a lost frame at the beginning of a session. However, if such a device's resynchronization mechanism is

to completely renegotiate CCP (as has been witnessed in testing with some vendors' devices), this sequence will repeat infinitely.

4. For SFVRA Database Users: you may enable (by checking) or disable the *Callback* option. When enabled, any Cabletron systems that receives a call from this user should disconnect and re-establish the connection. The returning call will be made by a system within the same group with at least two more free channels than the system receiving the incoming call, if applicable. Users must have a telephone number configured in order to enable this feature.

CONFIGURING PROTOCOL INFORMATION

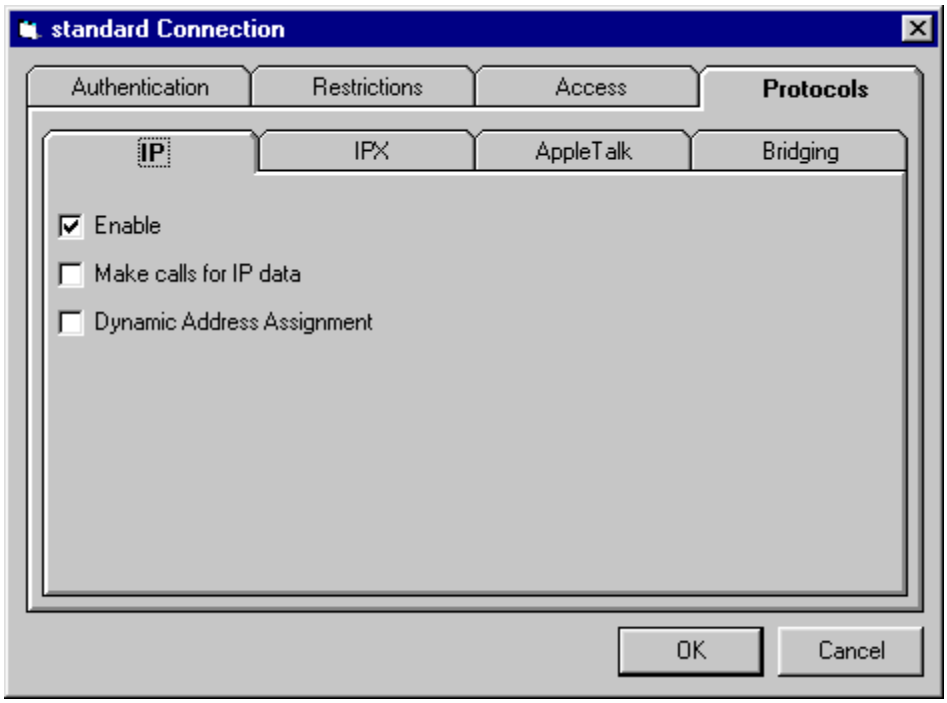
CyberSWITCH systems and 9W006/9W007 SmartSwitch Remote Access Modules can communicate using the following protocols:

- IP
- IPX
- AppleTalk
- Bridging

Refer to the following sections for completing protocol connection information.

CONFIGURING IP INFORMATION

1. Click on the *IP* tab to display the following IP dialog box.



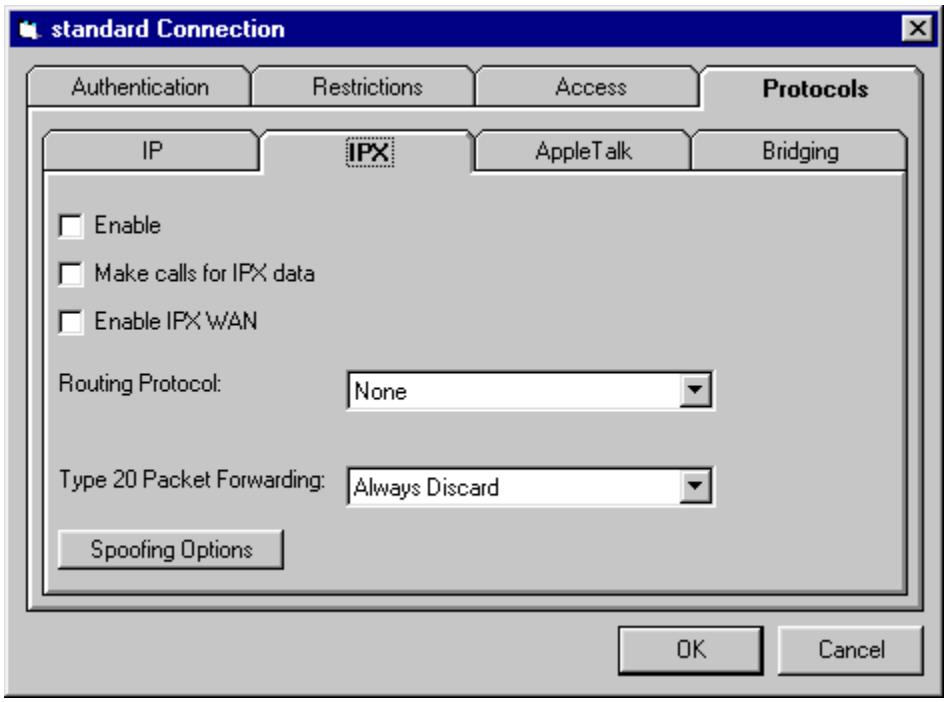
2. Check *Enable* to enable IP routing (as shown above).

3. To allow IP dial out, check *Make calls for IP data.*

4. If you would like IP addresses to be dynamically assigned, check *Dynamic Address Assignment*.

CONFIGURING IPX INFORMATION

1. Click on the *IPX* tab to display the following IPX dialog box.



2. Check *Enable* to enable IPX routing.

3. To allow IPX dial out, check *Make calls for IPX data*.

4. Check *Enable IPX WAN* if a site's system will be connected to a remote device that is an IPX router. This will ensure that IPX WAN protocol will immediately succeed IPXCP negotiations.

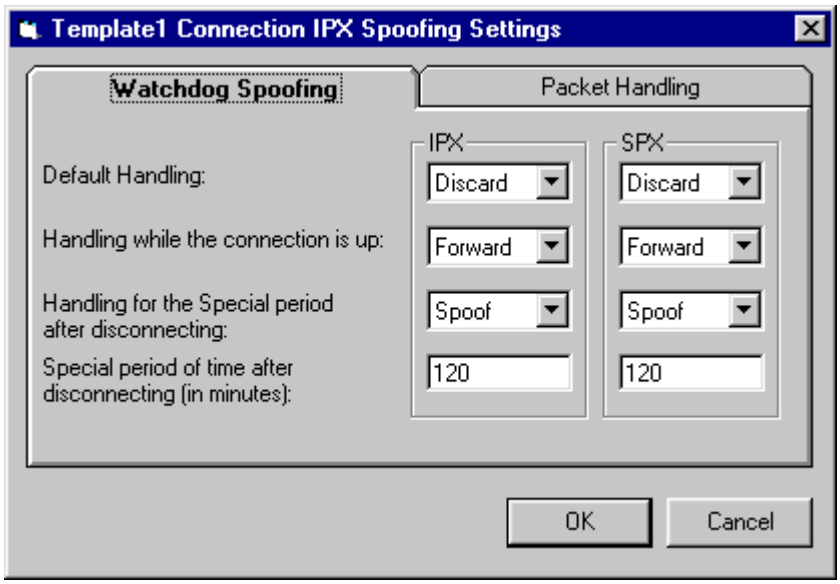
5. Select an IPX *Routing Protocol*. This is the protocol the remote device will be using to communicate with the Cabletron system. Available protocols are:
   - *None*
   - *RIP/SAP*
   - *Triggered RIP/SAP*

6. If you have selected *Triggered RIP/SAP* as the IPX routing protocol, you will need to select a *WAN Peer Type.* Choices are:
   - *Active:* an active WAN peer receives and sends information at all times.
   - *Passive*: a passive WAN peer receives / sends information only when a connection is up.

7. Select the *Type 20 Packet Forwarding* method. This allows you to control under what conditions IPX type 20 broadcast packets will be broadcasted. Choices are:
   - always discard
   - forward when user is connected
   - always forward

8. Configure the *Spoofing Options*. There are two categories of spoofing options: watchdog and packet handling.

   a. Configure *Watchdog Spoofing* information. The example below shows default values.



Watchdog Spoofing parameters include:

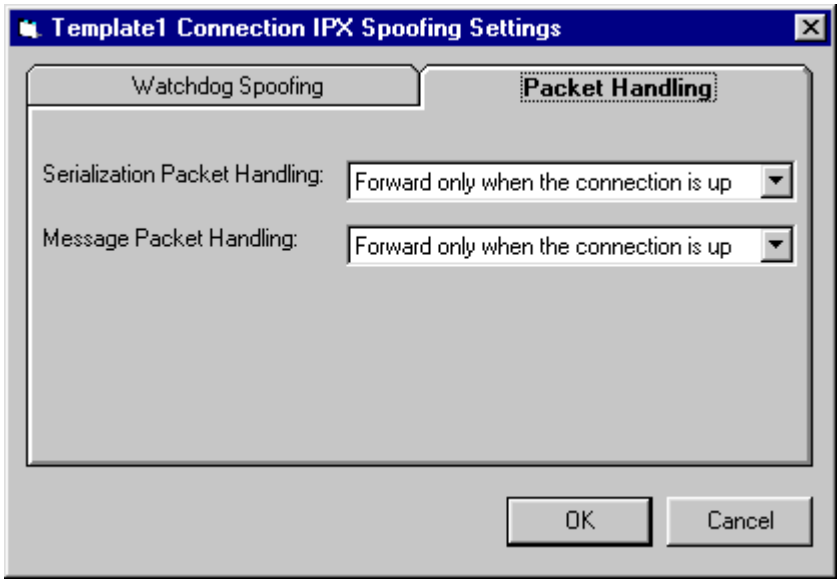
- *Default Handling*
  Allows you to control how IPX and SPX packets are handled as a default. You may select to forward, spoof, or discard IPX and SPX packets.

- *Handling while the connection is up*
  Allows you to control how IPX and SPX packets are handled while a connection is up. You may select to forward, spoof, or discard IPX packets while the connection is up. SPX packets must be forwarded while the connection is up.

- *Handling for the Special period after disconnecting*
  Allows you to control how IPX and SPX packets are handled during a configured grace period after disconnecting. You may select to forward, spoof, or discard IPX and SPX packets during this special handling period.

- *Special period of time after disconnecting (in minutes)*
  Allows you to set the grace period after disconnecting.

b. Configure the *Packet Handling* information. The example below shows default values.



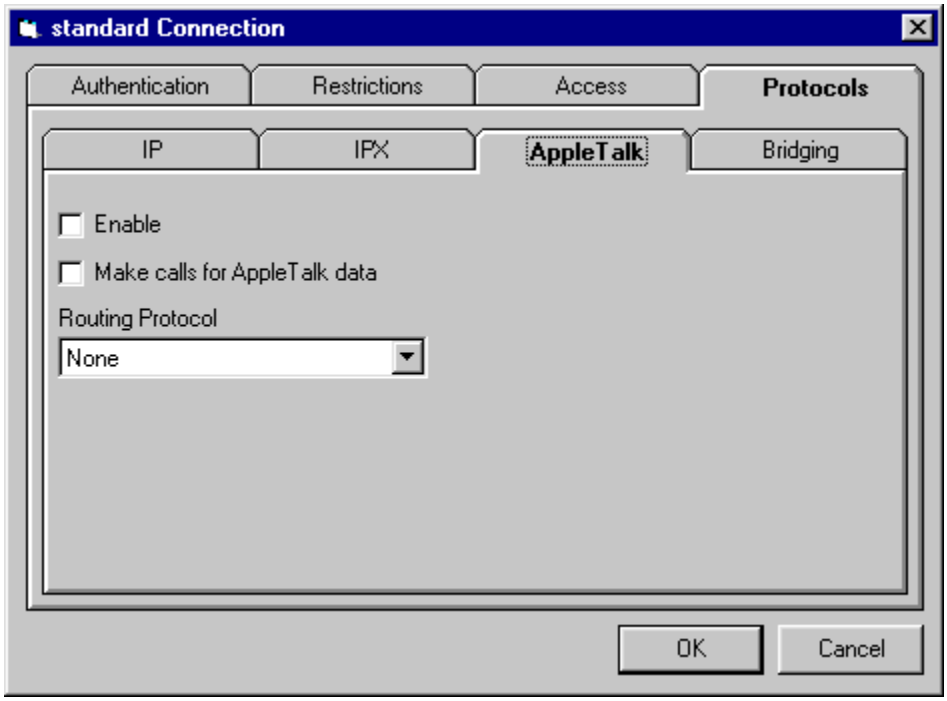
Packet handling parameters include:

- *Serialization Packet Handling*
  Allows you to control how serialization packets are handled. You may select to always discard, forward only when the connection is up, or always forward.

- *Message Packet Handling*
  Allows you to control how message packets are handled. You may select to always discard, forward only when the connection is up, or always forward.

CONFIGURING APPLETALK INFORMATION

1. Click on the *AppleTalk* tab to display the following AppleTalk dialog box.



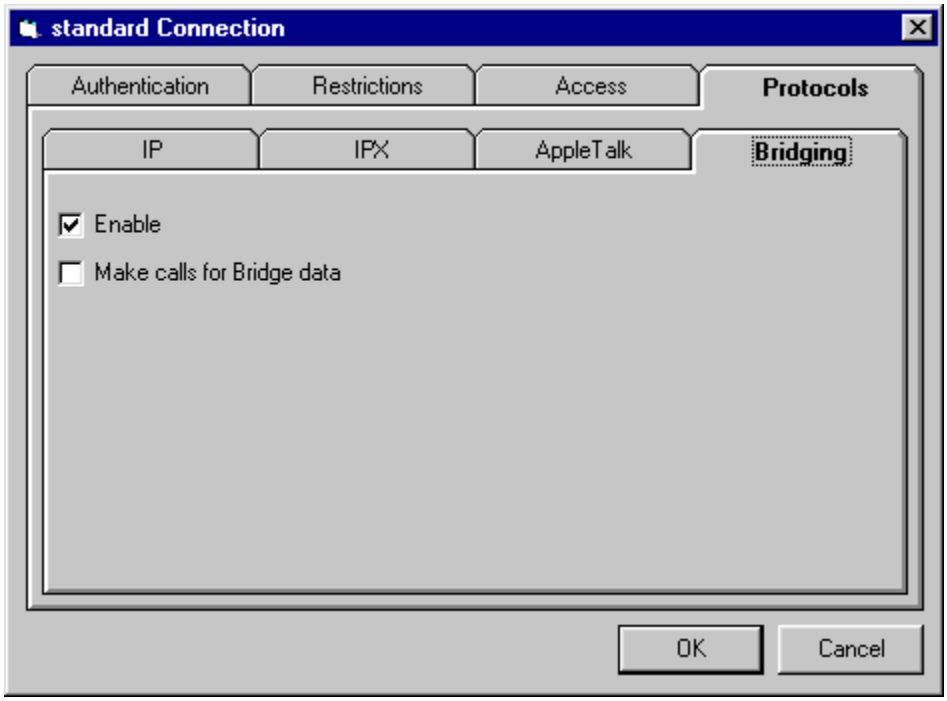
2. Check *Enable* to enable AppleTalk routing.

3. To allow AppleTalk dial out, check *Make calls for AppleTalk data.*

4. Select an AppleTalk *Routing Protocol*. This specifies the AppleTalk routing protocol the system should use with a remote device. The options are none or RTMP. Currently RTMP is only supported for users who will be dialing into a Cabletron system via a MAC dial-in port.

CONFIGURING BRIDGING INFORMATION

1. Click on the *Bridging* tab to display the following Bridging dialog box.



2. Check *Enable* to enable bridging.

3. To allow bridge dial out, check *Make calls for Bridge data*.

CONFIGURING SITES

OVERVIEW

After you have designed site templates (refer to Configuring Site Templates), you can then define individual sites. For each site you will enter various site properties (including the site template you wish to use for this site), optional contact information, and the systems associated with this site.

ADDING A SITE

The initial steps to configuring a site are as follows:

1. From the menu bar, click on *Functions* then click on *Sites*, or click on the toolbar.

2. Click on *Add*.

3. You can now configure site properties, contacts, and systems.

CONFIGURING SITE PROPERTIES

1. Enter a user-defined *Site Name* (maximum of 17 characters).

2. Select a *User Database* for user authentication. Choices are:
   - *Local User Table*
   - *SFVRA*
   - *Other* (for systems not configured by the SFVRA-CFG)

3. If you selected a Local User Table or SFVRA database, select a *Site Template* from the list of previously configured templates.

4. If you selected an SFVRA database, select a *Database Site* from the previously configured list. Refer to *Configuring the SFVRA Database Table* for instructions on configuring SFVRA database information.

5. Enter the *Device Authentication* information.

   a. Enter the site's device authentication *Name*. Note that multiple sites can use the same authentication name.

   b. If your site uses PAP security, enter the *User Password*.

   c. If your site uses CHAP security, enter the *CHAP Secret*.

6. If applicable, enter the site's *ISDN Subaddress*. A subaddress may be configured for a point-multipoint line.

7. If you are adding a site to a network that is already completely configured (i.e., connection groups have already been configured), you can select the site's *Connection Group* from the list

of previously configured connection groups. If you select a connection group, you may also opt to automatically add a connection from the site to the group's central site.

Otherwise, you will configure the connection group information at a later time (refer to *Configuring Connection Groups*).

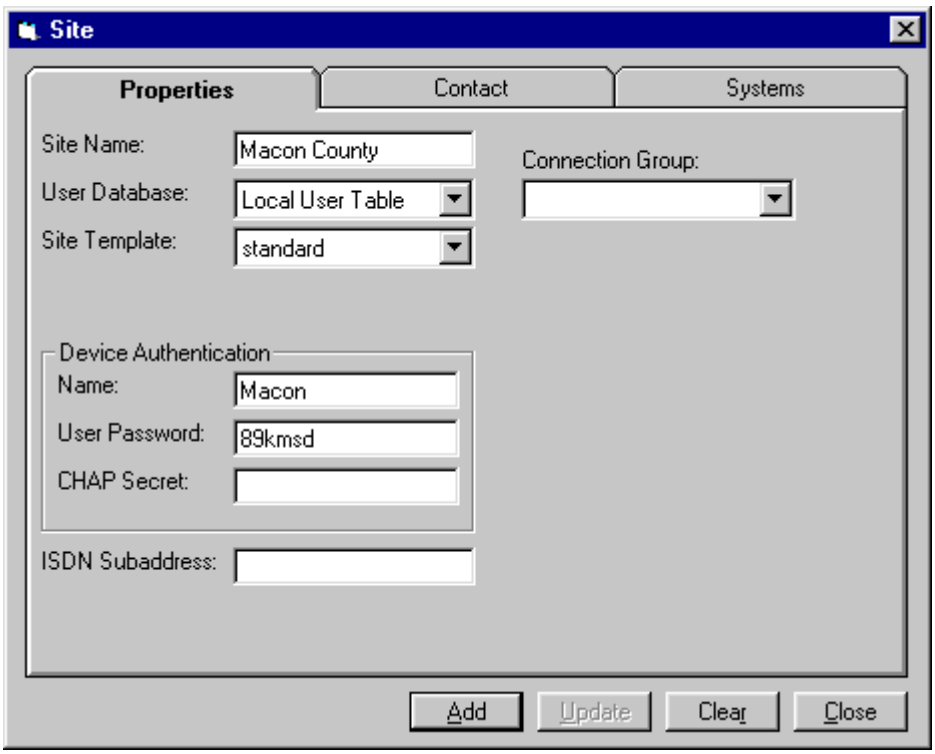
Note: It is sometimes advantageous to configure site systems before selecting a connection group. Directory and hunt group numbers configured for systems are used to initialize connection dial out phone numbers when a site is added to a connection group. So if you wait to add the connection group after the system's telephone information is configured (under the system's circuit information), the telephone numbers will automatically be incorporated into the connection group telephone information. Thus, this will save you from having to manually enter the telephone information.

8. If you have selected a Connection Group for this site, and the Connection Group *has* a configured central site, you may check *Add Connection to Central Site*. This will automatically add a connection from this site to the Connection Group's central site.

9. If you have selected a Connection Group for this site, and the Connection Group *does not have* a configured central site, you may check *Central Site*. This will automatically designate this site as the Connection Group's central site.

10. Click on *Add* to save the site properties.

An example site properties dialog box is shown below.



CONFIGURING CONTACT INFORMATION

Configuring *Contact* information is optional. To enter contact information, click on the *Contact* tab and enter contact information for the site.

CONFIGURING THE SITE'S SYSTEMS

To define the site's systems:

1. Click on the *Systems* tab.

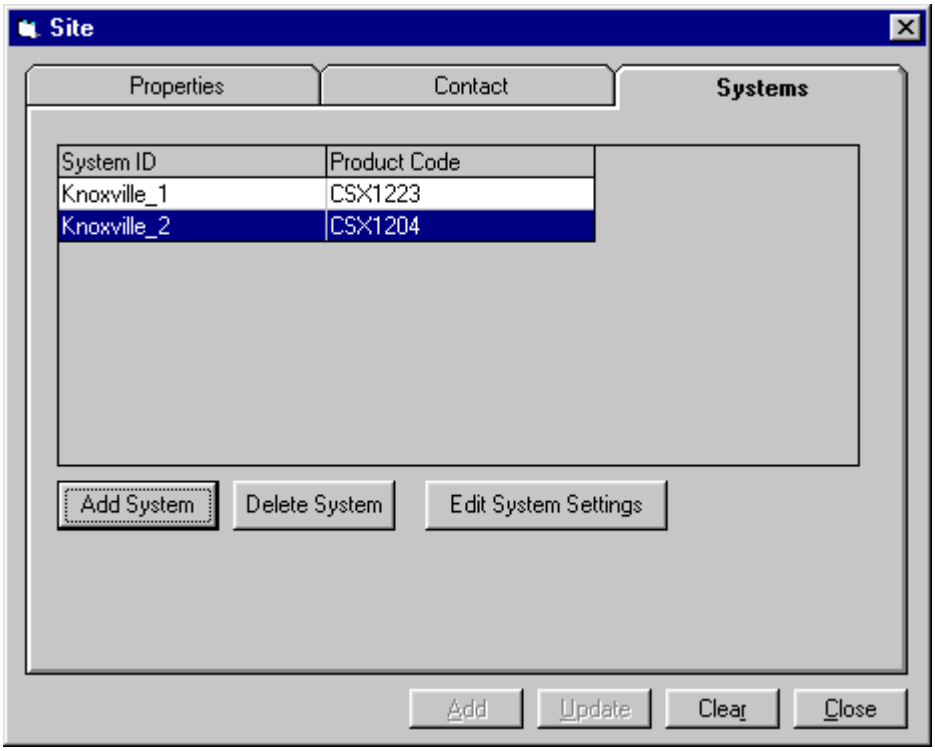
2. Click on *Add System*.

3. The *System ID* is predefined using the following format: [sitename_n], with a maximum of 18 characters. For example, the first system you add to site "Knoxville" will be assigned Knoxville_1, the second site will be Knoxville_2, etc.

   Note: If you have assigned a site name of more than 16 characters, the system ID will not be predefined. This is because the site name has a maximum of 18 character as does the system ID. So, for example, if you assign a site name of seventeen characters, there will not be enough free characters left to add [_n] to create the system ID (17 + 2 = 19, which exceeds the maximum number of characters allowed for a system ID). If the system ID is not predefined, you may enter a user-defined system ID.

4. Select the system's *Product Code*. For example, if the system is a CyberSWITCH 1223, you would select CSX1223 from the product code list.

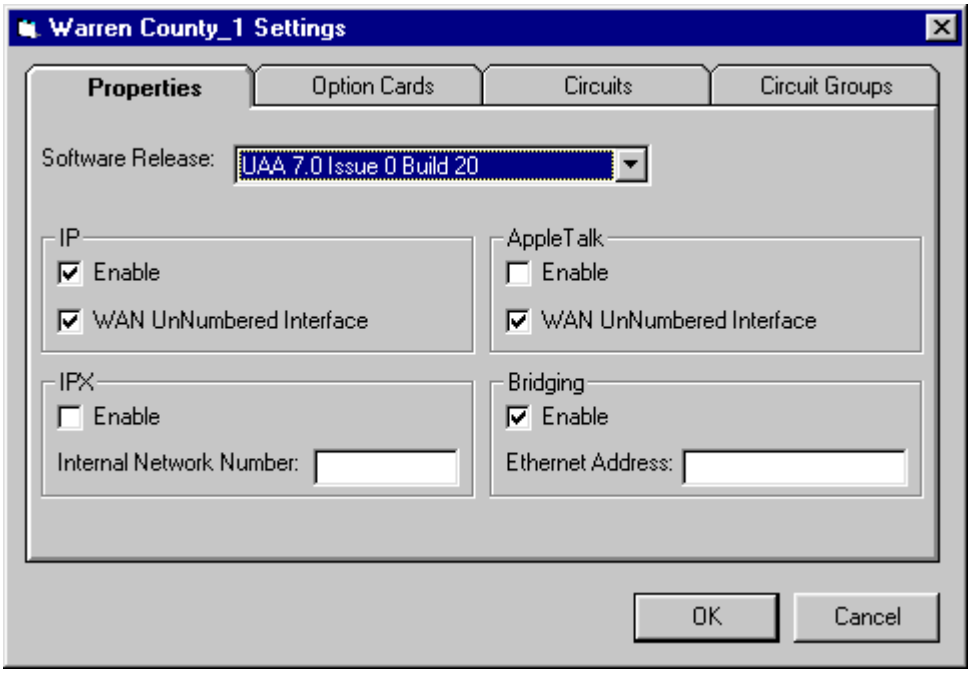
5. Click on *Add*. You should now see a screen similar to the following example screen:



6. Repeat steps 2 through 5 to add additional systems to the site.

7. To configure additional system information, click on the system's *System ID* (or on the *Product Code*), then click on *Edit System Settings*. (Double clicking on the System ID or on the Product Code will also display the screen for entering additional system information.) From the resulting screen (example shown below) you can configure system *Properties, Option Cards* (only for PC-based platforms), *Circuits, and Circuit Groups* information.

   Note: If the product code you select is *CSX100* or *Modem User*, you will only be able to enter the system's Ethernet address.



a. *Properties* information:

- *Software Release*
  Select the software release that the Cabletron system is running.

- *IP Information*
  You may *enable* or *disable* IP routing on a per system basis. Also, you may select to use a *WAN UnNumbered Interface*.

- *IPX Information*
  You may *enable* or *disable* IPX routing on a per system basis. If IPX is enabled for this system, enter the system's *Internal Network Number*. This number uniquely identifies a specific IPX router in the internetwork. In the Novell environment, an IPX internal network number must be assigned to all IPX routers. This number is an arbitrary value, assigned when the IPX router is configured. It may be 1 to 8 hexadecimal digits in length (up to 4 bytes).

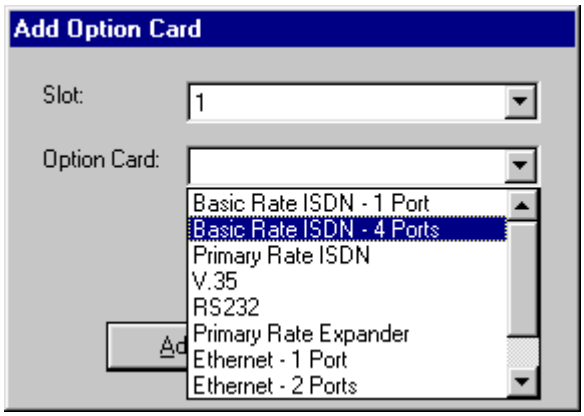
- *AppleTalk Information*
  You may *enable* or *disable* AppleTalk routing on a per system basis. Also, you may select to use a *WAN UnNumbered Interface*.

- *Bridging Information*
  You may *enable* or *disable* bridging on a per system basis. If this system has bridging enabled and will be using Bridge MAC Address Security, enter the system's *Ethernet Address*.

b. *Options Cards* information (for PC-based platforms only):

You may add or delete option cards to the system's configuration. To add an option card:

- Click on *Add Option Card.*
- Select the *Slot* number the option card is installed in.
- Select the *Option Card* type. In the example screen shown below, we are configuring a 4 port BRI option card to be in slot 1.



- Click on *Add.*

c. *Circuits* information:

You may enter or edit *Circuits* information here, through the *Site* menu bar selection. The same circuit information is also configurable through the *Circuits* menu bar selection (see *Configuring Circuits*). In both places, the exact same information is entered. The difference is that the Site circuit dialog box focuses on the individual system, whereas if you access the circuit information through the Circuits menu bar selection, you look at the circuit configuration for all of the network's systems.

To configure the system's circuit information here:

- Click on the *Circuits* tab.
- Click on the specific slot / port you are interested in, then click on *Edit Circuit*. (Double clicking on your selection will also display the screen for entering circuit information.)
- Refer to *Configuring Circuits* for instructions for entering circuit information.

d. *Circuit Groups* information:

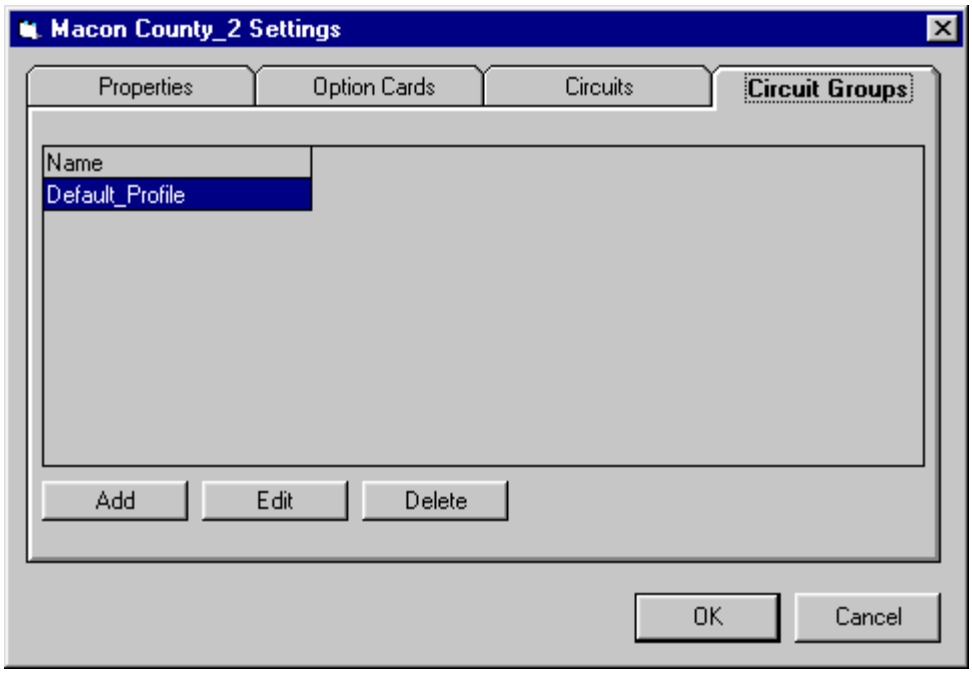
You configure system information for the Bandwidth Reservation feature under this heading. Bandwidth Reservation allows a portion of the possible connections (circuits) to always be available to specific users for both inbound and outbound calls. To increase flexibility, this feature may be configured to either allow or prevent bandwidth overlap. Bandwidth overlap will allow normal users to use a certain number of circuits (lines), while a special class of super users would be allowed access to both the normal bandwidth (designated in the default profile) as well as special super user bandwidth (designated in the configured user profile). "No overlap" would restrict each set of users to their own circuits.

When configuring your bandwidth reservation, consider the following:

- This is a BRI-only feature since bandwidth is reserved per-circuit.
- It is necessary to reject calls from users who have mistakenly called in on a circuit reserved for other user(s).
- Outbound calls are also restricted to the circuits reserved for a user.
- When Bandwidth Reservation is disabled, any user can connect on any circuit.
- When Bandwidth Reservation is enabled, a default profile list of circuits will be configured for use by all users that are not configured to use an alternate profile in the reserved list. This default profile list may be configured to remove circuits from general use.

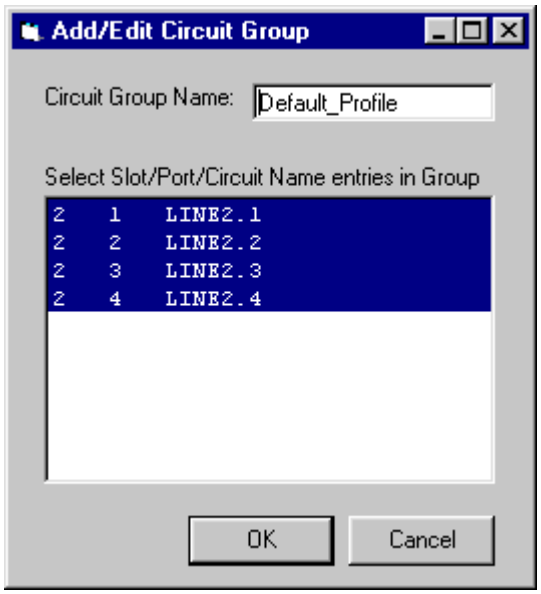
To customize the default profile:

- Click on the *Circuit Groups* tab. A screen similar to the following will be displayed:



- To designate the Default Profile:

  Select *Default_Profile*, then click on *Edit* (or simply double click on *Default_Profile*). A screen similar to the following will be displayed:



  As stated earlier, circuits configured under the default profile are available for all valid users. As shown above, the default profile initially shows all of the slot's BRI circuits to be selected. You may "unselect" the circuits you do not want available for the default profile. For example, if you want all valid users to have access to circuits LINE2.1 and LINE2.2, but not to LINE2.3 and LINE2.4, click on LINE2.3 and LINE2.4 so that they are no longer highlighted. Then click on *OK*.

- To add an alternate circuit group, click on *Add*. Enter a *Circuit Group Name*. Highlight the circuits you want available for this group. Click on *OK*.

Later, when configuring Connection Groups, you may designate a connection's circuit group from a list of available circuit groups.

CONFIGURING CIRCUITS

OVERVIEW

Circuits are the physical WAN connections to each system. Circuit information includes line properties, and where applicable, data link and access information.

A large portion of the circuits configuration information is automatically incorporated from the site template associated with the system. As discussed in earlier chapters, first you create site templates, then, when configuring a site, you associate a site template with the site. In result, each of the site's systems are also associated with a site template.

This chapter provides information to help you edit existing circuit information.

INITIAL STEPS

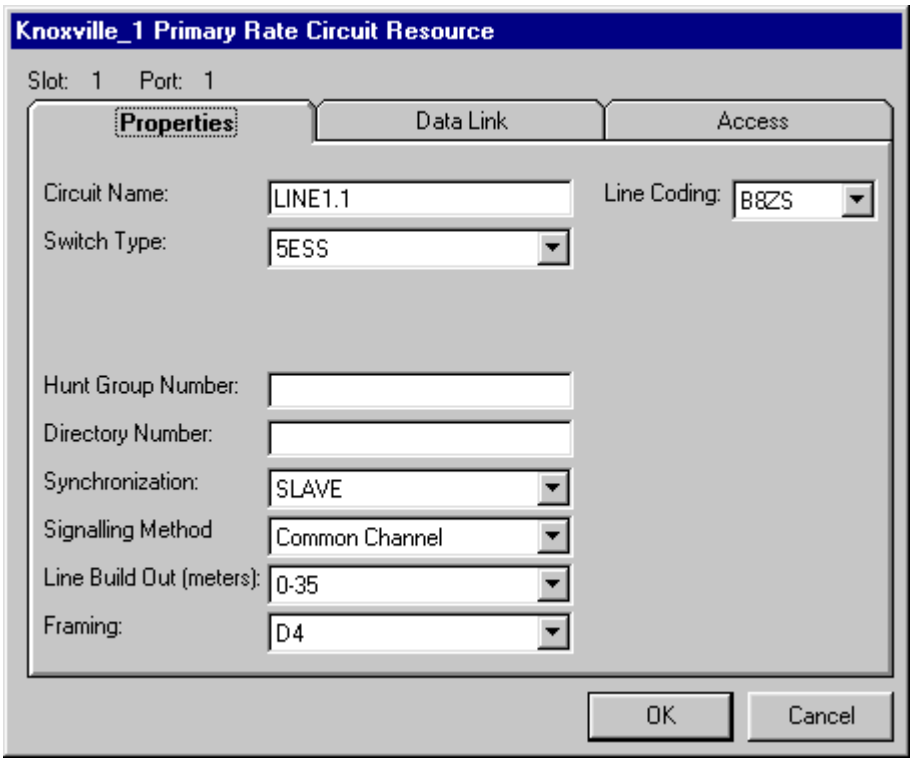
The initial steps to configuring circuit information are as follows:

1. From the menu bar, click on *Functions* then click on *Circuits*, or click on the toolbar.

2. To edit circuit information, click on the table entry pertaining to the desired circuit, then click on *Select*. (Double clicking on the table entry will also display the same screen.) Depending on resource type, from the resulting screen you may need to configure information for all or some of the following: circuit *Properties*, *Data Links*, *Call Screening*, and *Access* information.

CONFIGURING CIRCUIT PROPERTIES

The example screen below shows basic property information for a PRI 5ESS circuit. All of the shown configured values were automatically incorporated from the site template associated with the system.



If the circuit's configuration varies from the values taken from the site template, you can edit these values.

Notice that there are also blank fields: *Hunt Group Number* and *Directory Number*. Depending on the configuration needed for the system, you may want to enter information in these fields. These fields are defined as follows:

- *Hunt Group Number*
  Only available for BRI or PRI circuits. A hunt group is a series of telephone lines organized in such a way that if the first line is busy the next line is hunted and so on until a free line is found. The hunt group number is the telephone number used for this circuit's hunt group.

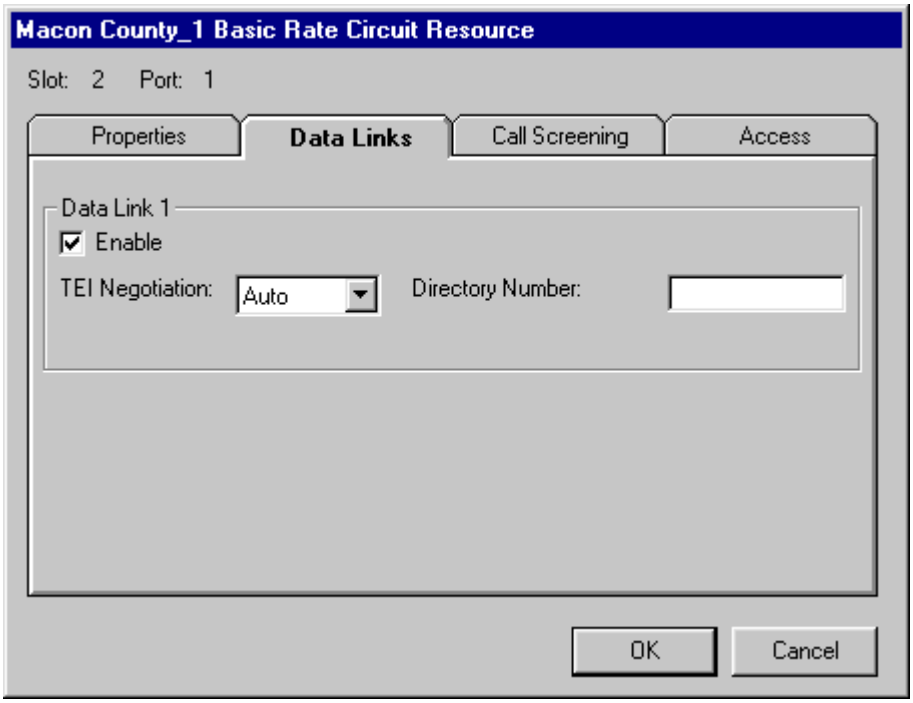
- *Directory Number*
  Only available for PRI circuits. (A BRI circuit's directory number is configured under the Data Links tab.) This is the telephone number used for this circuit. When connection groups are formed, this number is used for initial population of the phone list. For example, if you configure a directory number for Site1, then create a connection group containing Site1 and a second site, Site2, Site2 would add Site1's directory number to its list of numbers to use to connect to Site1.

Notes: These numbers will populate the telephone numbers for the connection groups. You may need to modify these telephone numbers under the connection group telephone information if prefixes are needed. For example, if the dial out call is a long distance call, you will need to add a 1 and the area code, or, if the system has a Centrex system you will need to add a 9 before the number.

Also note that once you configure the connection group, all new phone numbers or modifications to old phone numbers must be done through the connection group; changes made to the circuit information will not be reflected under the previously configured connection group information.

CONFIGURING CIRCUIT DATA LINKS

Only for BRI and PRI circuits. All of the shown configured values were automatically incorporated from the site template associated with the system.



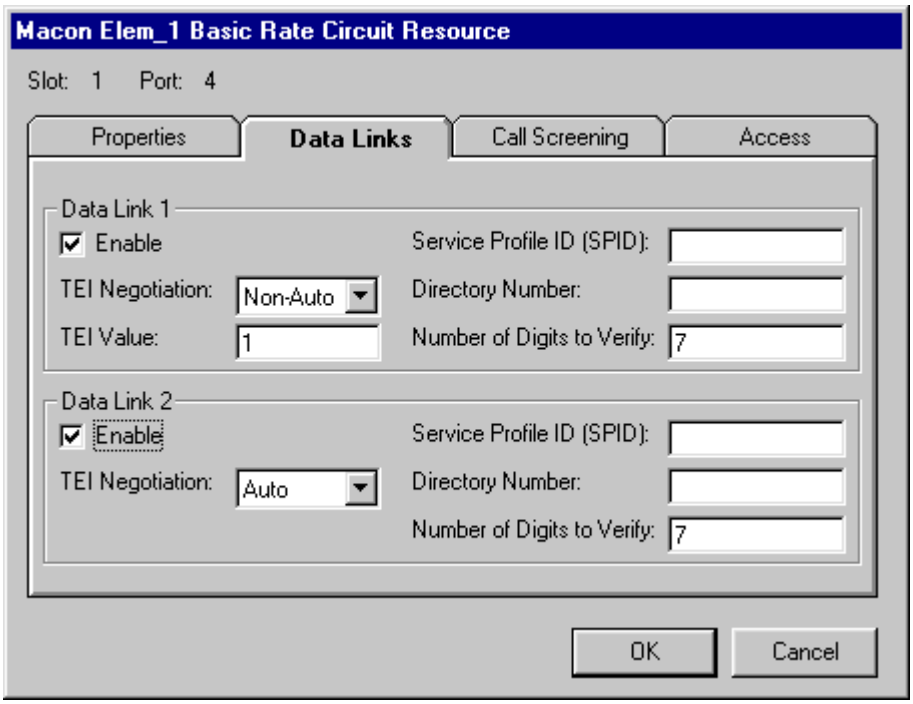
If the circuit's configuration varies from the values taken from the site template, you can edit these values.

TEI Negotiation and TEI Value fields may be included for both BRI and PRI circuits. When configuring data links for BRI circuits, extra fields are included.

Additional BRI circuit information:

- *Enable/Disable Data Links*
  Only for BRI circuits. Data links may be disabled completely for all BRI switch types except DMS100 and NI-1. This is often done when dedicated lines are in use.

- *SPID Information*
  If a BRI circuit uses a DMS100 or NI-1 switch type, the Data Link dialog box will require SPID information as shown below:



  SPID information includes: a *SPID*, a *Directory Number*, and the *Number of Digits to Verify*. The SPID is paired with a directory number to define a data link (see directory number definition below). The number of digits to verify (starting at the rightmost digit) helps to determine on which bearer to accept the phone call. The maximum number of digits is equal to the number of digits in the directory number.

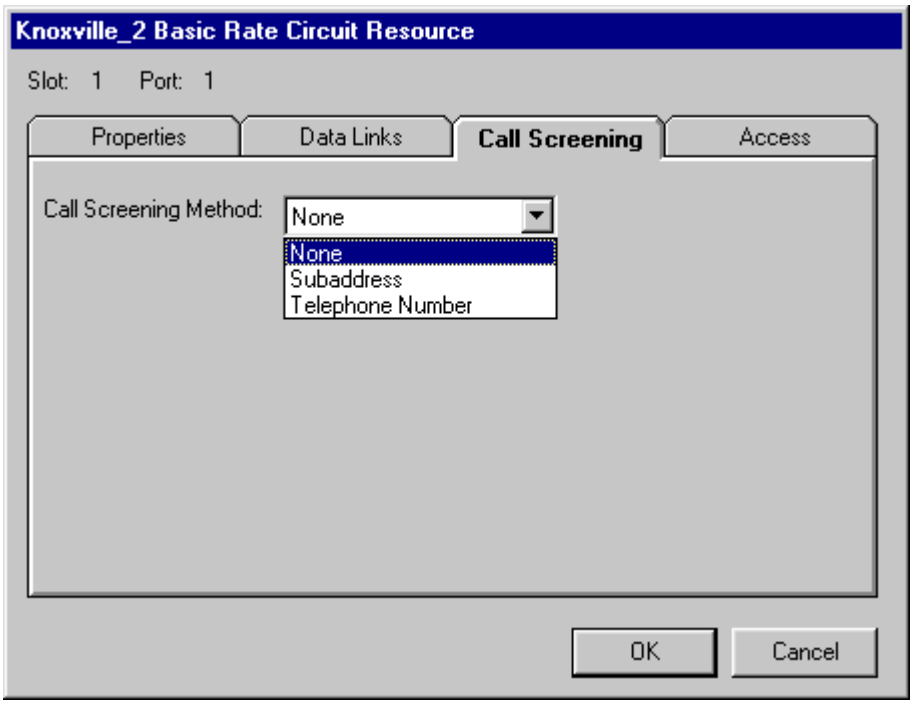
- *Directory Number*
  The directory number is similar for a BRI and a PRI circuit in that it is the telephone number used for this circuit. When connection groups are formed, this number is used for initial population of the phone list. But for a BRI circuit, the directory number serves a second purpose for circuits using DMS100 or NI-1 switch types. For these switch types, the directory number is also paired with the SPID number.

  Notes: These numbers will populate the telephone numbers for the connection groups. You may need to modify these telephone numbers under the connection group telephone information if prefixes are needed. For example, if the dial out call is a long distance call, you will need to add a 1 and the area code, or, if the system has a Centrex system you will need to add a 9 before the number.

  Also note that once you configure the connection group, all new phone numbers or modifications to old phone numbers must be done through the connection group; changes made to the circuit information will not be reflected under the previously configured connection group information.

CONFIGURING CIRCUIT CALL SCREENING

For BRI circuits only. If the circuit is a point-multipoint circuit, you can select one of the following call screening methods: none, subaddress, or telephone number (see example screen below).



Call screening methods are defined as follows:

- *None*
  All calls will be accepted.

- *Subaddress*
  Uses a configured subaddress for this site. To use this call screening method, you must have a subaddress configured for the circuit's site.

- *Telephone Number*
  Telephone number(s) for your site used for call screening. Only calls directed to that specific telephone number will be accepted. You also need to enter the maximum number of digits (starting at the rightmost digit) to be verified.

CONFIGURING CIRCUIT ACCESSES

An access defines the connection details the system uses to reach the network. CyberSWITCH systems and 9W006/9W007 SmartSwitch Remote Access Modules default to ISDN accesses (a

switched-network access). Configuring circuit access information allows you to configure the circuit to have a dedicated access.

To add a dedicated access:

1. Click on the *Access* tab.

2. Click on *Add Dedicated Access*.

3. Enter a user-defined *Access Name*.

4. Select the *Line Protocol* used by the access. Choices are:
   - PPP
   - HDLC

5. For PRI, V.35, and RS232 circuits: select the *Data Rate*.

6. For BRI and PRI circuits: select the *Bearer Channels* that will be used by the access.

7. For V.35 and RS232 circuits: select the *Clocking Type*. Choices are:
   - Internal
   - External

8. Click on *OK*.

CONFIGURING CONNECTION GROUPS

OVERVIEW

Through connection groups, you can divide a network into groups of sites that need to intercommunicate. Within each group, you can select a central site for the group, creating a star configuration.

This chapter provides instructions for:

- Adding Connection Groups
  This section provides instructions for forming connection groups from the list of configured sites.

- Modifying Star Configurations
  For some connection groups, the standard star configuration will need to be altered. This section provides instructions for modifying a star configuration.

- Modifying Connection Information
  There are various connection information elements that you may need to modify. For example, not all sites use the same telephone system. Centrex systems require a 9 for a prefix. Also, some sites require Calling Line IDs (CLIDs) for security. There are a few additional elements you will also need to consider. This section provides instructions for modifying connection information.

ADDING CONNECTION GROUPS

To add a connection group:

1. From the menu bar, click on *Functions* then click on *Connection Groups*, or click on the toolbar.

2. Click on *Add*.

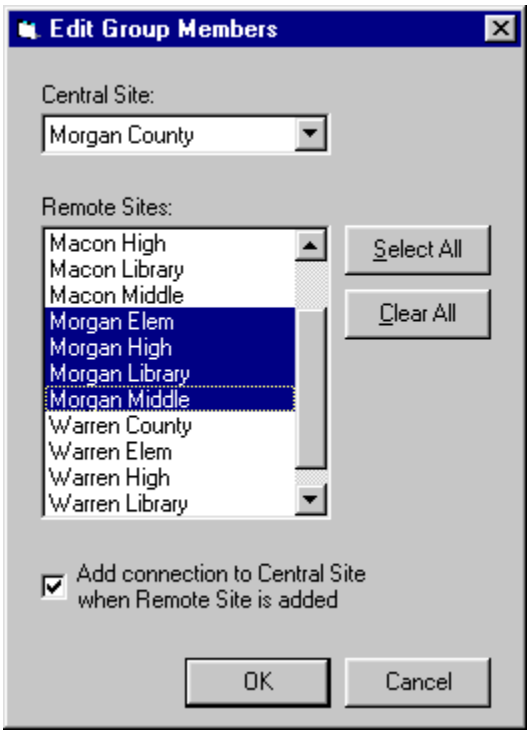
3. Enter a user-defined group name.

4. Click on *Add*.

5. To define group members, click on *Edit Group Members*.

6. Select a *Central Site* by clicking on the Central Site down arrow, then clicking on a site name from the displayed list.

7. Select the *Remote Sites* that will connect to the central site. Do this by clicking on the desired site names. As shown below, the sites you have selected will be highlighted after they are selected.



If all sites are remote sites, click on *Select All*. To clear the sites you have selected, click on *Clear All*.

8. To automatically configure a connection between the remote sites and the central site, make sure there is a check next to *Add connection to Central Site when Remote Site is added*. This will result in a star type configuration. It is also possible to edit the configuration so that it is not a standard star configuration. Refer to *Modifying Star Configurations* for instructions.

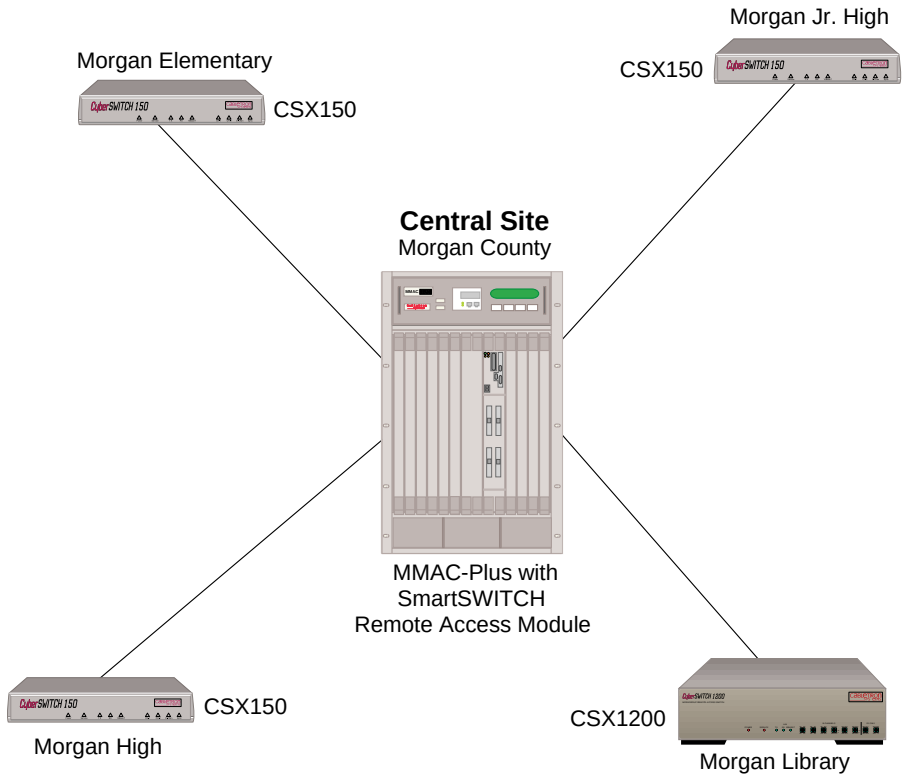
9. To add more connection groups, click on *OK*, then click on *Clear*, then repeat steps 3 through 8.

It is convenient to enter BRI circuit and PRI circuit directory numbers and hunt groups before adding connections. Refer to *Configuring Circuit Properties* and *Configuring Circuit Data Links* for instructions for configuring directory and hunt group numbers. When directory numbers and hunt group numbers are configured for circuits before connections are configured, then connection dial out phone numbers will automatically be set when the connection is added. Changes should not be necessary for most of this information, with two exceptions. You may need to adjust dial-out numbers, and, if the connection uses CLID security, you will need to enter Calling Line IDs. Instructions for making these changes are included in *Modifying Connection Information*.

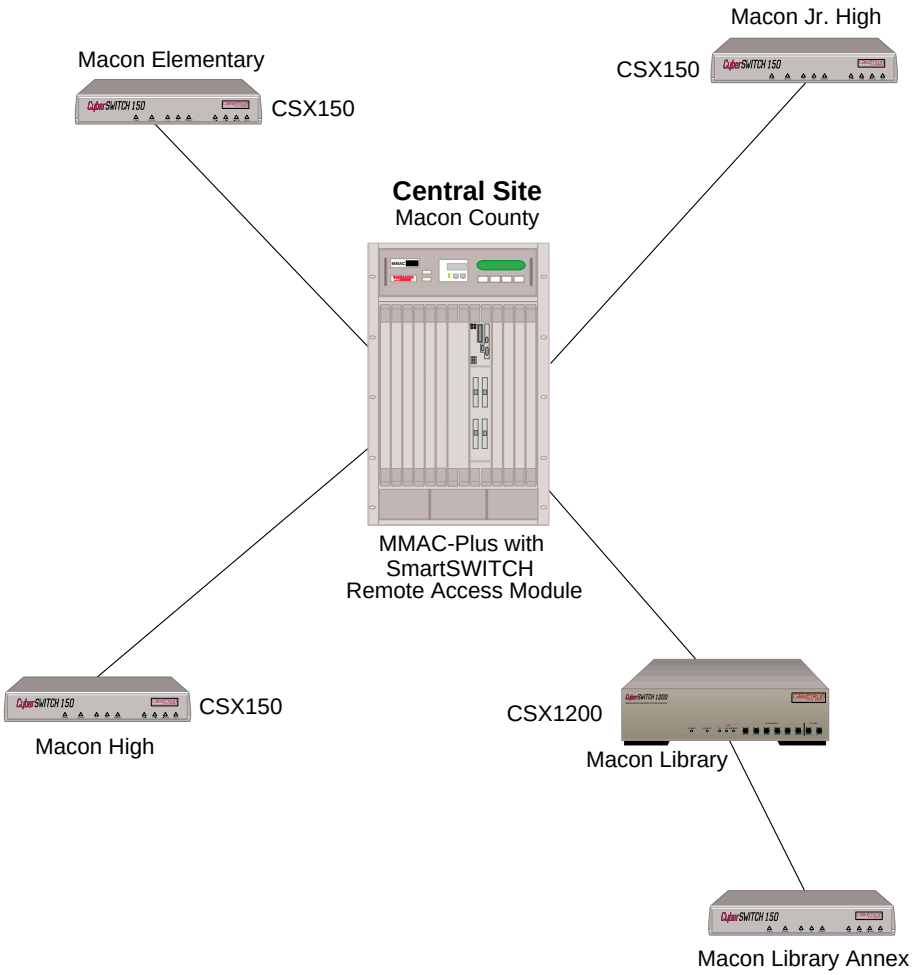
Note: Once you configure the connection group, all new phone numbers or modifications to old phone numbers must be done through the connection group; changes made to the circuit information will not be reflected under the previously configured connection group information.

MODIFYING STAR CONFIGURATIONS

When you choose to have a connection automatically configured between the remote sites and the central site, the result is a star network configuration. In a star network each remote device is connected to a central device. In the following example, site Morgan County is the central site in the star network.

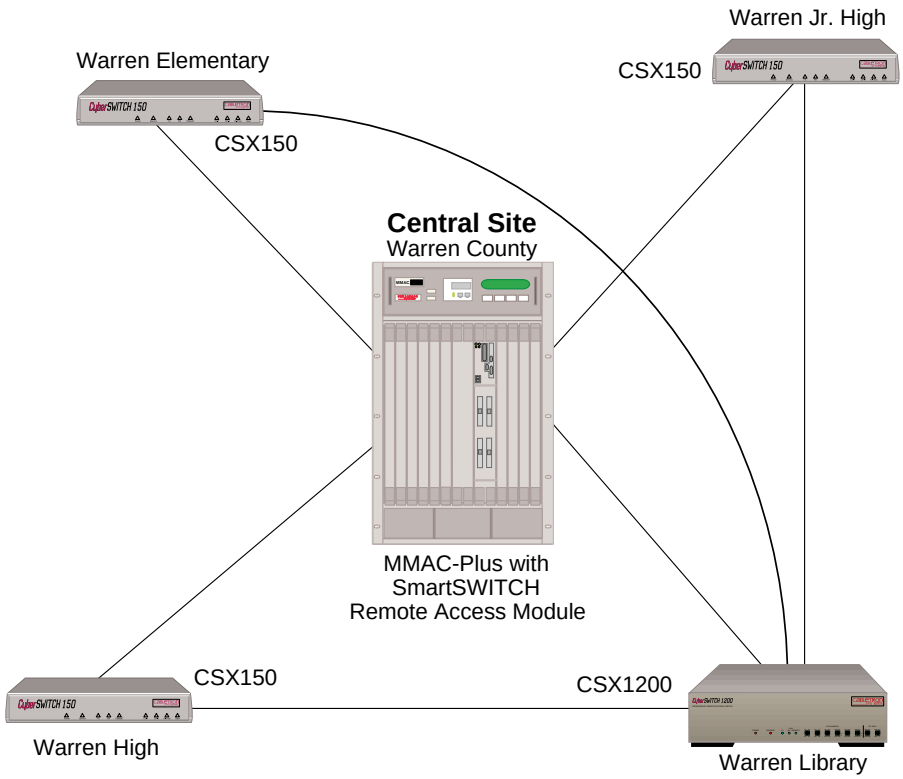


There may be situations where you may need to modify the star configuration to suit your network. For example, in the extended star network shown below, there is a library annex site (site Macon Library Annex) that only needs a direct connection to the library (site Macon Library). The annex does not need a direct connection to the central site (Morgan County).



Example 1: Extended Star

In our second example of a modified star network, a mesh network, there is a central site that needs to be connected to each school and to the library, and each school also needs a direct connection to the library.

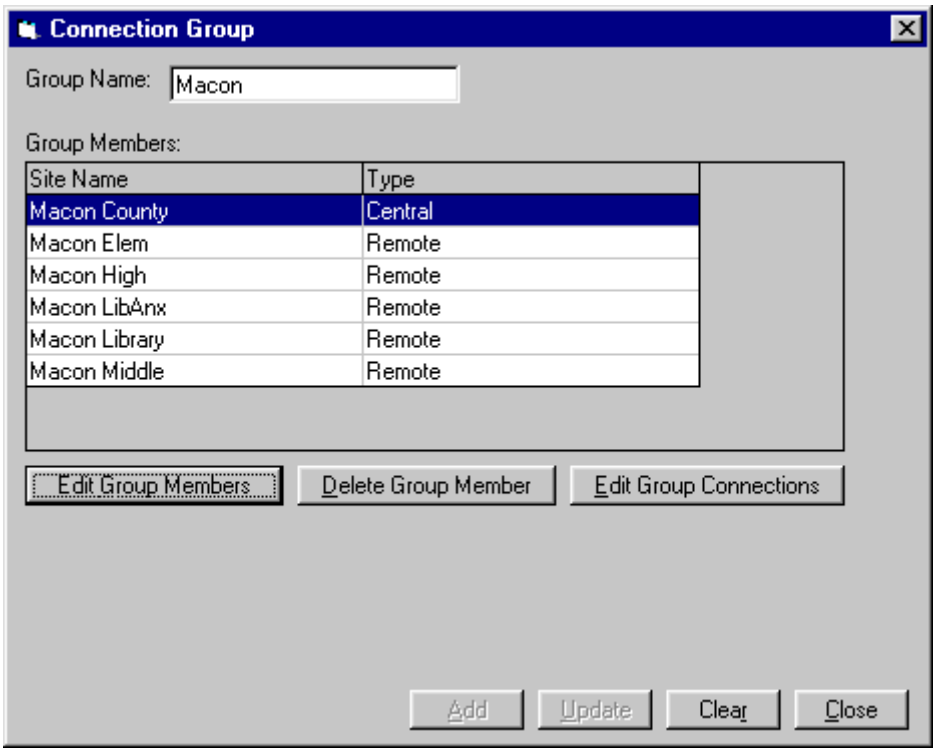


Example 2: Mesh Network

You can modify a standard star network configuration in one of two ways. We use Example 1 to illustrate both methods:

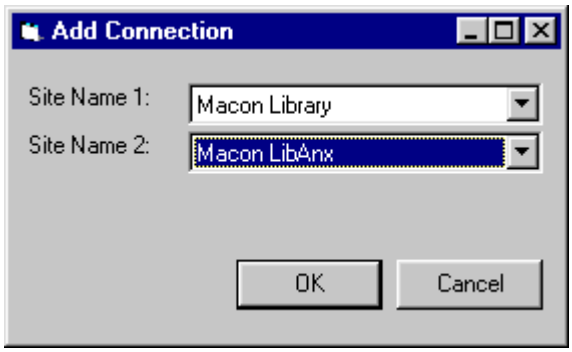
1. Add the site that is modifying the star configuration separately (For Example 1, that would be the library annex). When you add the site to the already configured connection group, do not select *Add connection to Central Site when Remote site is added*. Connection information will *not* automatically be established. You can then manually configure the connection information. To manually configure the information:

a. From the *Connection Group* screen (shown below), click on *Edit Group Connections.*



b. From the resulting *[Site Name] Connections* screen, click on *Add.*

c. From the resulting *Add Connection* screen, select the Site IDs of the two sites for which you want to configure a connection. As per Example 1, in the example screen below we configure a connection between Macon Library and Macon Library Annex.



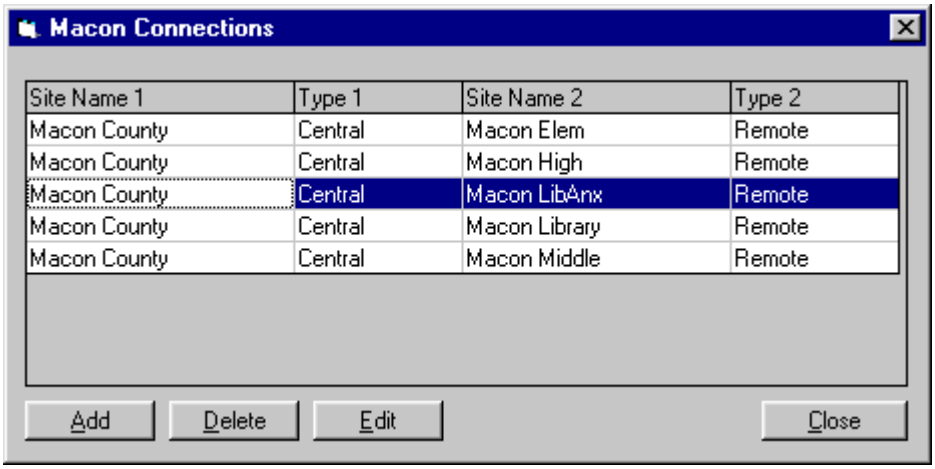
d. Click on *OK.*

2. With the second method, we assume that you added sites to the connection group with *Add connection to Central Site when Remote site is added* selected (hence, automatically establishes

connection information). You can then later change the connection information for the site that is modifying the star configuration. To modify the connection information:

a. As in step 1a above, from the *Connection Group* screen, click on *Edit Group Connections*.

b. Click on the connection that needs to be modified. In Example 1 we want to modify the connection between site Macon County and site Macon_LibAnx.

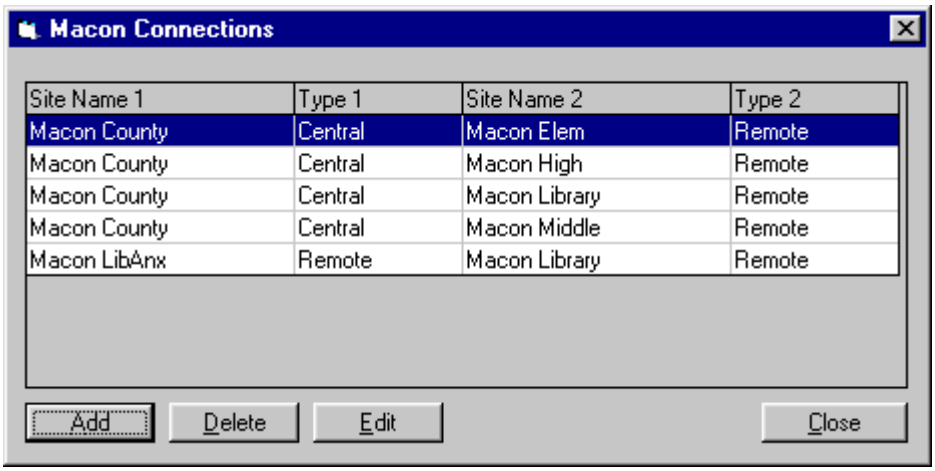


c. As stated earlier, the library annex does not need a direct connection to Macon County, it only needs to be connected to the library. Click on *Delete* to delete the connection.

d. We now want to add a connection from the library annex to the library. Click on *Add*.

e. From the resulting *Add Connection* screen, select the Site IDs of the two sites for which you want to configure a connection (these would be IDs for Macon Library and Macon Library Annex).

f. Click on *OK*. The screen will reflect the new connection information as shown below:



MODIFYING CONNECTION INFORMATION

For each connection configured, there is default information that was extracted from the site template associated with the system's site, and also from previously configured circuit information (e.g., Authentication, Restriction, Access, and Protocol information). Changes should not be necessary for most of this information, with the following exceptions.

- You may need to adjust dial-out numbers (e.g., you may need to add a prefix to the number).
- If the connection uses CLID security, you will need to enter Calling Line IDs.
- If you are using the Bandwidth Reservation feature for this connection group, you will need to select the appropriate circuit group.
- If IP is enabled on the connection, an IP Subnet must be selected.
- If AppleTalk is enabled on the connection, an AppleTalk segment must be selected.

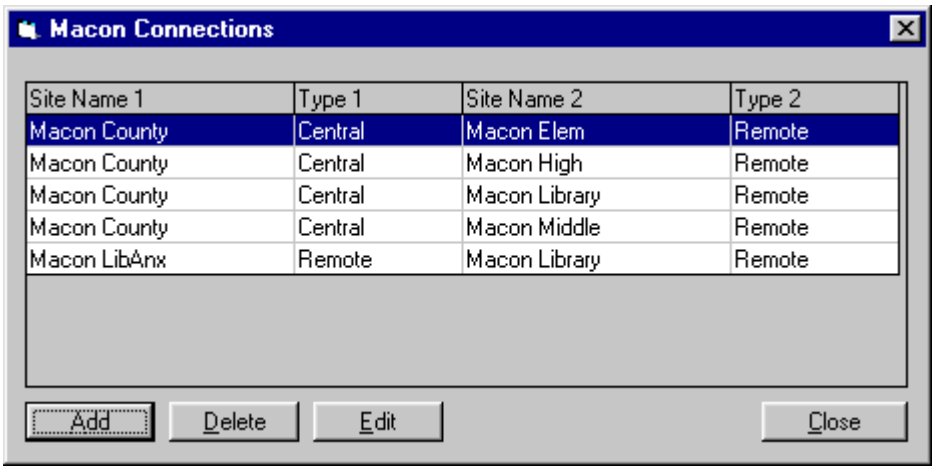
ADJUSTING TELEPHONE NUMBERS

To adjust connection telephone numbers:

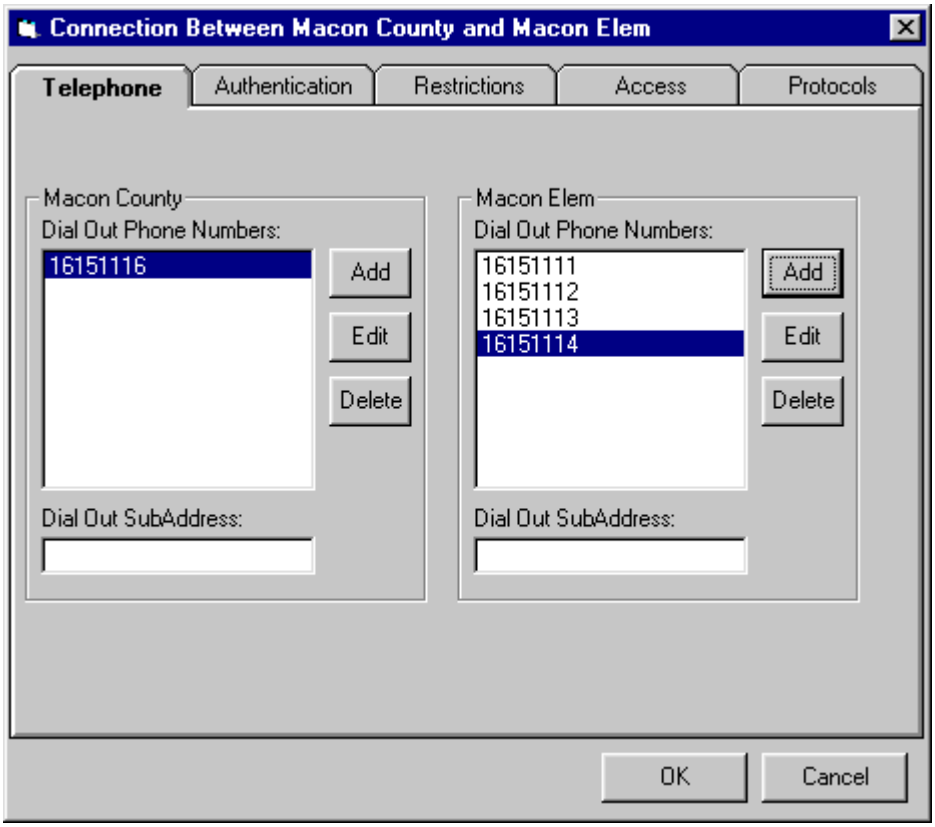
1. From the Connection Groups' main dialog box, click on the *Connection Group Name* that is associated with the telephone number you want to change, then click on *Select* (or simply double click on the Connection Group Name).

2. From the resulting screen, click on *Edit Group Connections.*

3. From the resulting [Site Name] Connections screen, click on the particular connection that you want to make the changes to, then click *Edit* (or simply double click on the connection). In the screen shown below, we are selecting the connection between Macon County and Macon Elementary.



4. The resulting screen will display the connection's telephone information as shown below.

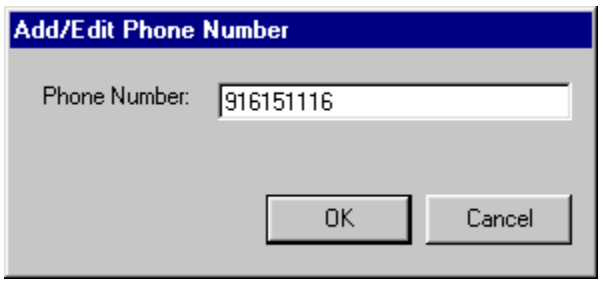


5. From this screen you may add, edit, or delete phone numbers. For explanation purposes, let us say that both sites have a Centrex system. So, when calling out to these sites you must first dial a 9. We need to add a 9 to each telephone number. To edit the numbers to include a 9:

   a. Highlight the number we want to change (by clicking on it).

   b. Click on *Edit*, the existing phone number will be displayed.

   c. Insert a 9 before the telephone number (as shown below), then click on *OK*.



   d. Repeat steps a through c for each number you need to adjust.

ENTERING CALLING LINE IDS

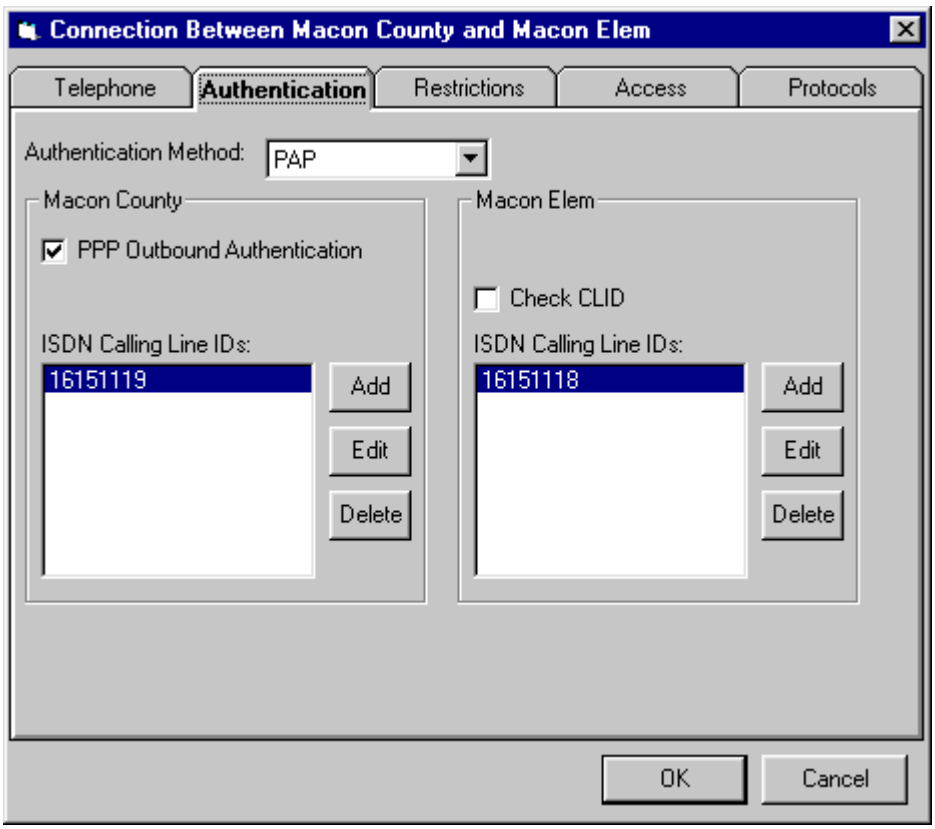
Calling Line IDs (CLIDs) are applicable only if CLID is enabled at the site level (see *Configuring Authentication Information*). Once CLID is enabled, you can then enter CLIDs for specific connections. To configure a CLID for a connection:

1. From the Connection Groups' main dialog box, click on the *Connection Group Name* that is associated with the connection for which you want to add a CLID, then click on *Select* (or simply double click on the Connection Group Name).

2. From the resulting screen, click on *Edit Group Connections.*

3. From the resulting *[Site Name] Connections* screen, click on the particular connection that you want to make the changes to, then click *Edit* (or simply double click on the connection).

4. From the resulting screen, click on the *Authentication* tab. You will then see a screen similar to the following:

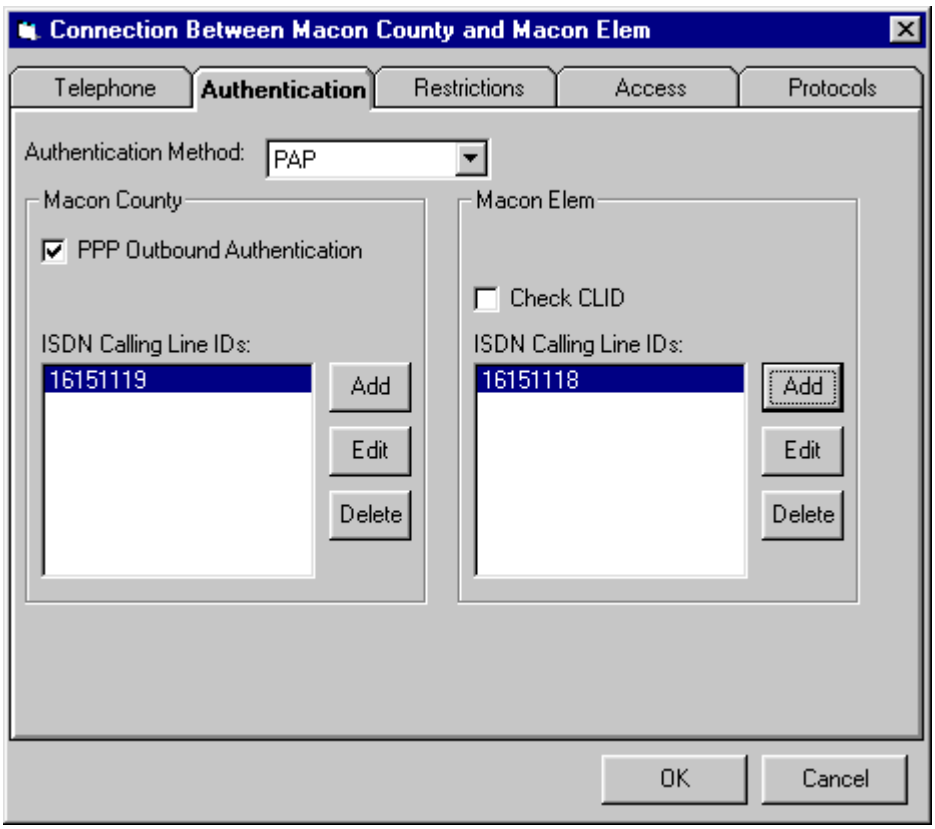


In the above example, Site Macon County uses a local user database, whereas site Macon Elem uses an SFVRA database. Keeping this in mind, note the following:

- You need to select an *Authentication Method*. This is only required if at least one of the two sites uses an SFVRA database.

- You may enable (with a check) PPP Outbound Authentication for sites using a local user database.
- You may require that the site's CLID be checked when a connection is made for the site(s) using an SFVRA database.

5. From the above screen you may add, edit, or delete CLIDs. To add a CLID, click on *Add*, then enter the CLID. Repeat for each required CLID. When done, click on *OK*. Remember that the CLID is another device's telephone number from whom this site will accept a call from. For example, as shown by the screen below, Macon Library will accept calls from Macon_LibAnx if the calls come in on the following number: 16151119; and Macon_LibAnx will accept calls from Macon Library if the calls come in on the following number: 16151118.



ADJUSTING RESTRICTION INFORMATION

Normally, the restriction information should not have to be adjusted. If you do need to adjust any of the restriction information:

1. From the Connection Groups' main dialog box, click on the *Connection Group Name* that is associated with the connection for which you want to modify the protocol information, then click on *Select* (or simply double click on the Connection Group Name).

2. From the resulting screen, click on *Edit Group Connections*.

3. From the resulting *[Site Name] Connections* screen, click on the particular connection that you want to make the changes to, then click *Edit* (or simply double click on the connection).

4. From the resulting screen, click on the *Restrictions* tab. Make the necessary configuration changes, then click *OK*.

ADJUSTING ACCESS INFORMATION

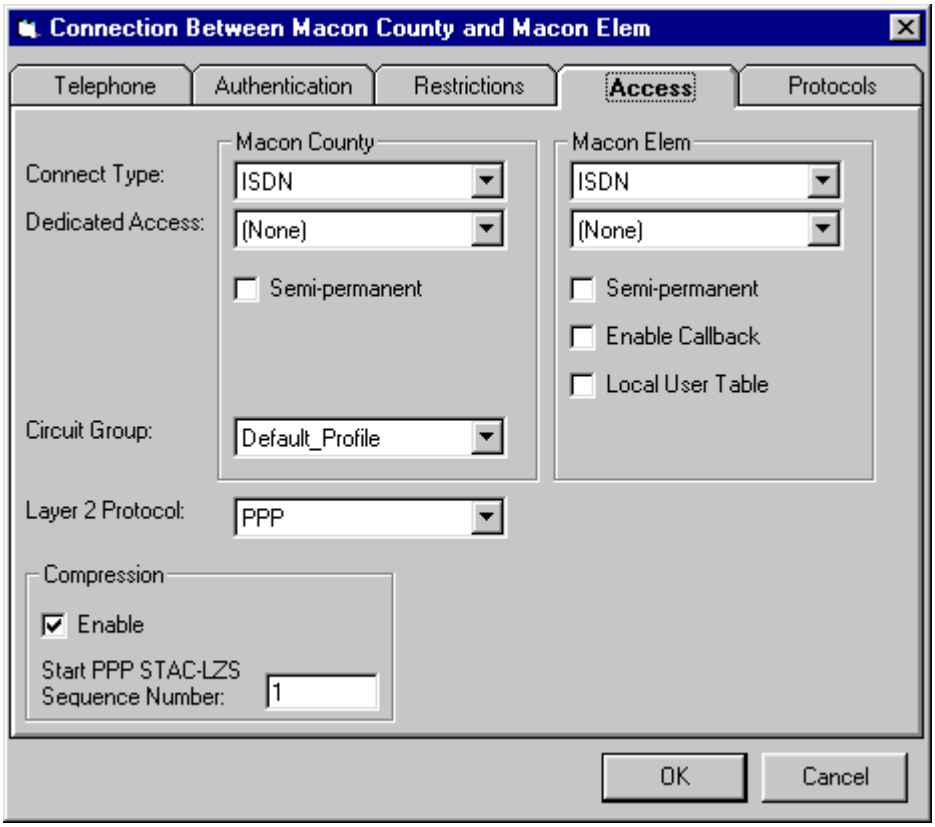
If you are using the Bandwidth Reservation feature for this connection group, you will need to select the appropriate circuit group. The circuit group is selected under the *Access* tab. To select a circuit group for the connection:

1. From the Connection Groups' main dialog box, click on the *Connection Group Name* that is associated with the connection for which you want to modify the protocol information, then click on *Select* (or simply double click on the Connection Group Name).

2. From the resulting screen, click on *Edit Group Connections*.

3. From the resulting *[Site Name] Connections* screen, click on the particular connection that you want to make the changes to, then click *Edit* (or simply double click on the connection).

4. From the resulting screen, click on the *Access* tab. You will then see a screen similar to the following:



5. Select the *Circuit Group* that you want to associate with this connection group. In the above screen, both sites use the default profile.

ADJUSTING PROTOCOL INFORMATION

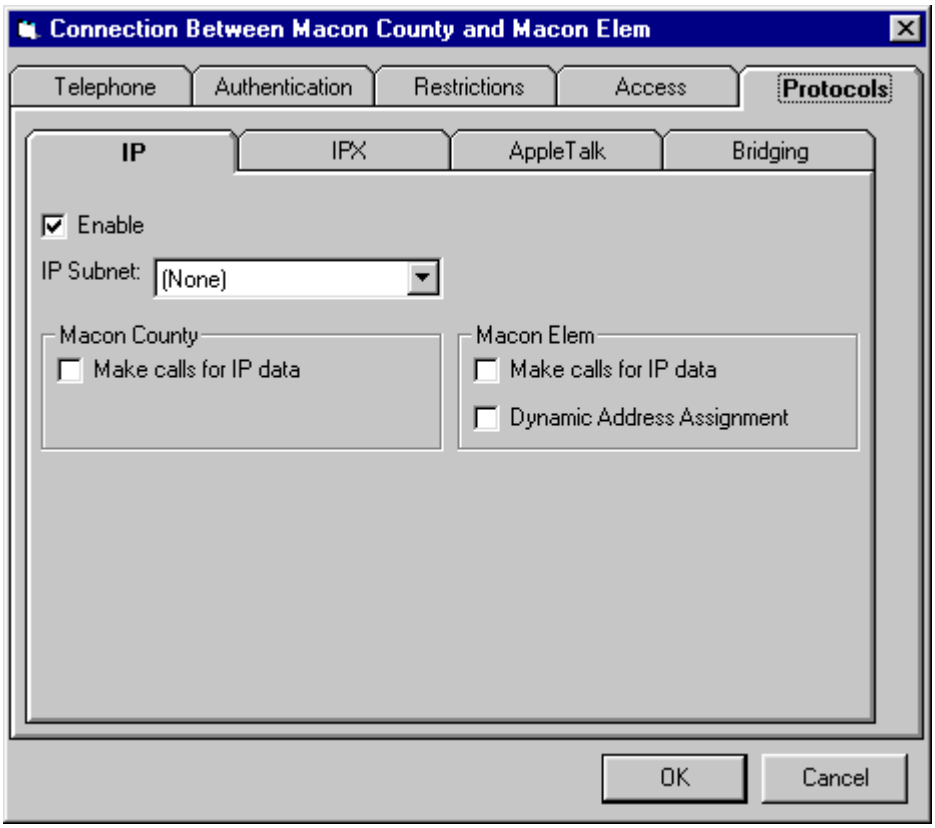
If you have enabled IP or AppleTalk protocol for this connection, then you will need to adjust the connection information to reflect the correct IP subnet or AppleTalk segment associated with this connection. Both IP and AppleTalk information is located under the connection *Protocols* information. To adjust this information:

1. From the Connection Groups' main dialog box, click on the *Connection Group Name* that is associated with the connection for which you want to modify the protocol information, then click on *Select* (or simply double click on the Connection Group Name).

2. From the resulting screen, click on *Edit Group Connections.*

3. From the resulting *[Site Name] Connections* screen, click on the particular connection that you want to make the changes to, then click *Edit* (or simply double click on the connection).

4. From the resulting screen, click on the *Protocols* tab. You will then see the following screen:



5. If this connection uses IP, make sure there is a check mark by *Enable.* Select the IP Subnet associated with this connection from the IP screen shown above. Also, under *IP Subnet* select *(UnNumbered)* if the connection uses an IP WAN UnNumbered interface.

6. If this connection uses AppleTalk, click on the AppleTalk tab, then from the resulting screen make sure there is a check mark by *Enable*. Select the AppleTalk Segment associated with this connection. Also, under *AppleTalk Segment* select *(UnNumbered)* if the connection uses an AppleTalk WAN UnNumbered interface.

CONFIGURING IP NETWORK INFORMATION

OVERVIEW

The IP protocol defines and routes datagrams across the network and provides connectionless transport service. It uses packet switching and makes a best effort to deliver its packets. The IP protocol uses the services of the data-link layer to accomplish the actual transmission.

The IP protocol was designed to handle the interconnection of the vast number of internet WAN and LAN networks. The SFVRA-CFG's IP network information defines how an IP network will interconnect. The network interface information you configure defines a system's network connections. The static route information you configure defines routes to networks across a WAN, or to LAN networks through a router that does not support IP RIP.

You can configure or view IP network information in one of two ways: at the subnet level or at the system level. The subnet view looks at IP network information with the "big picture" in mind; you are viewing how multiple systems interconnect to form a subnet. The system view looks at IP information with a specific system in mind; you are viewing how the individual system relates to the rest of the network.

Depending on which view you will be using to add IP network information, refer to one of the following two sections for instructions:

- *Configuring IP Network Subnet Information*
- *Configuring IP Network System Information*

Both views share basic concepts. These concepts are described in *IP Network Concepts*.

Note: Although you cannot currently use SFVRA-CFG to configure IP filters, you may use the device's CFGEDIT utility to configure filters. You can then go back to using SFVRA-CFG as your configuration tool *as long as you have made no other changes using CFGEDIT*. At the end of this chapter we provide special information regarding configuring IP filters.

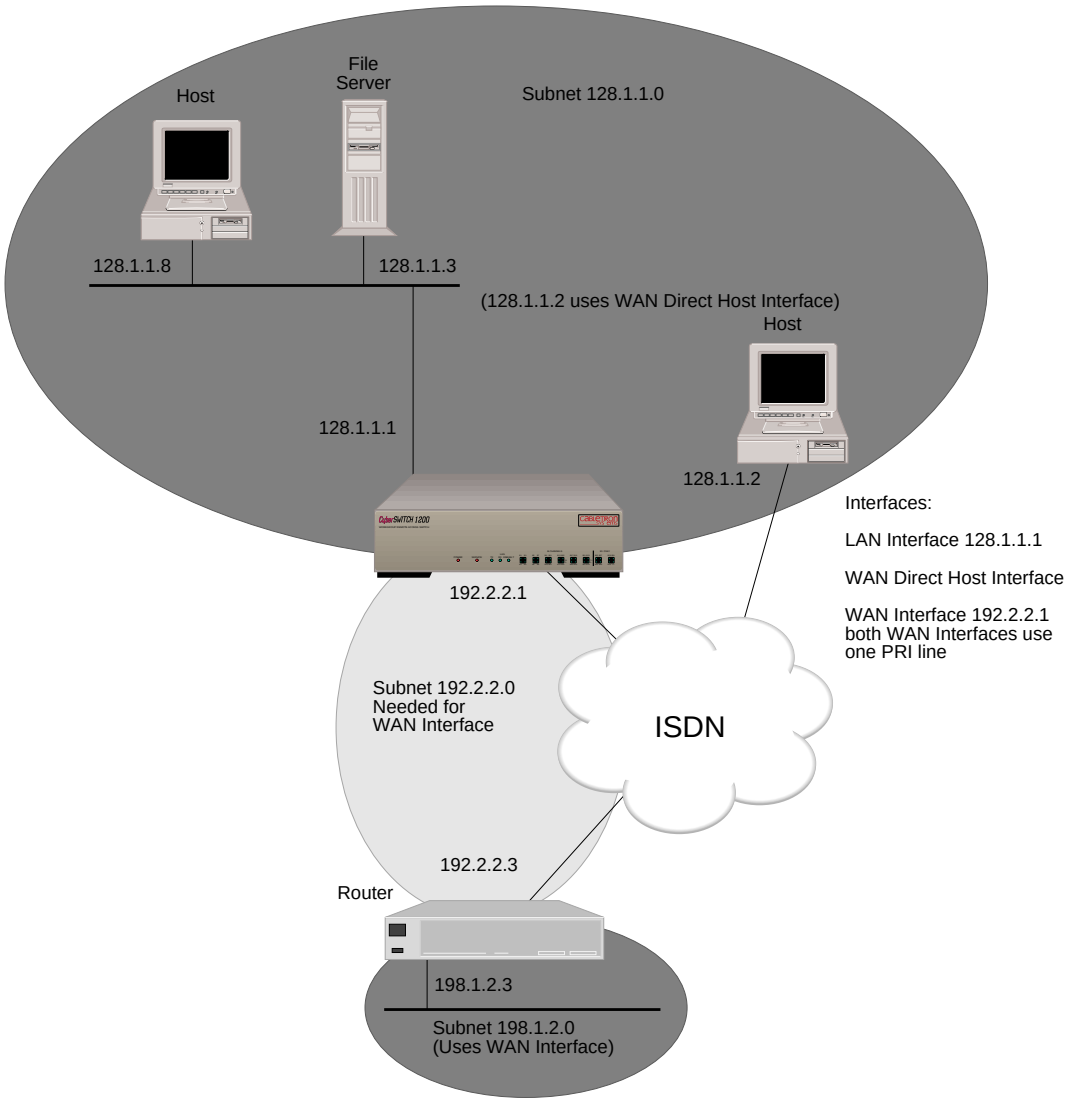
IP NETWORK CONCEPTS

Regardless of how you add IP network information, there are two main concepts you need to understand: network interfaces and static routes. In the following sections, we provide an overview of each concept.

NETWORK INTERFACES

Network interfaces are the connections of a system to a data network. For example, the Ethernet resource provides a network interface to a Ethernet LAN. The ISDN lines provide network interfaces to multiple remote networks. Because of their switched nature, the ISDN lines provide virtual network interfaces. That is, the same physical ISDN line can actually connect to different remote networks by dialing a different phone number.

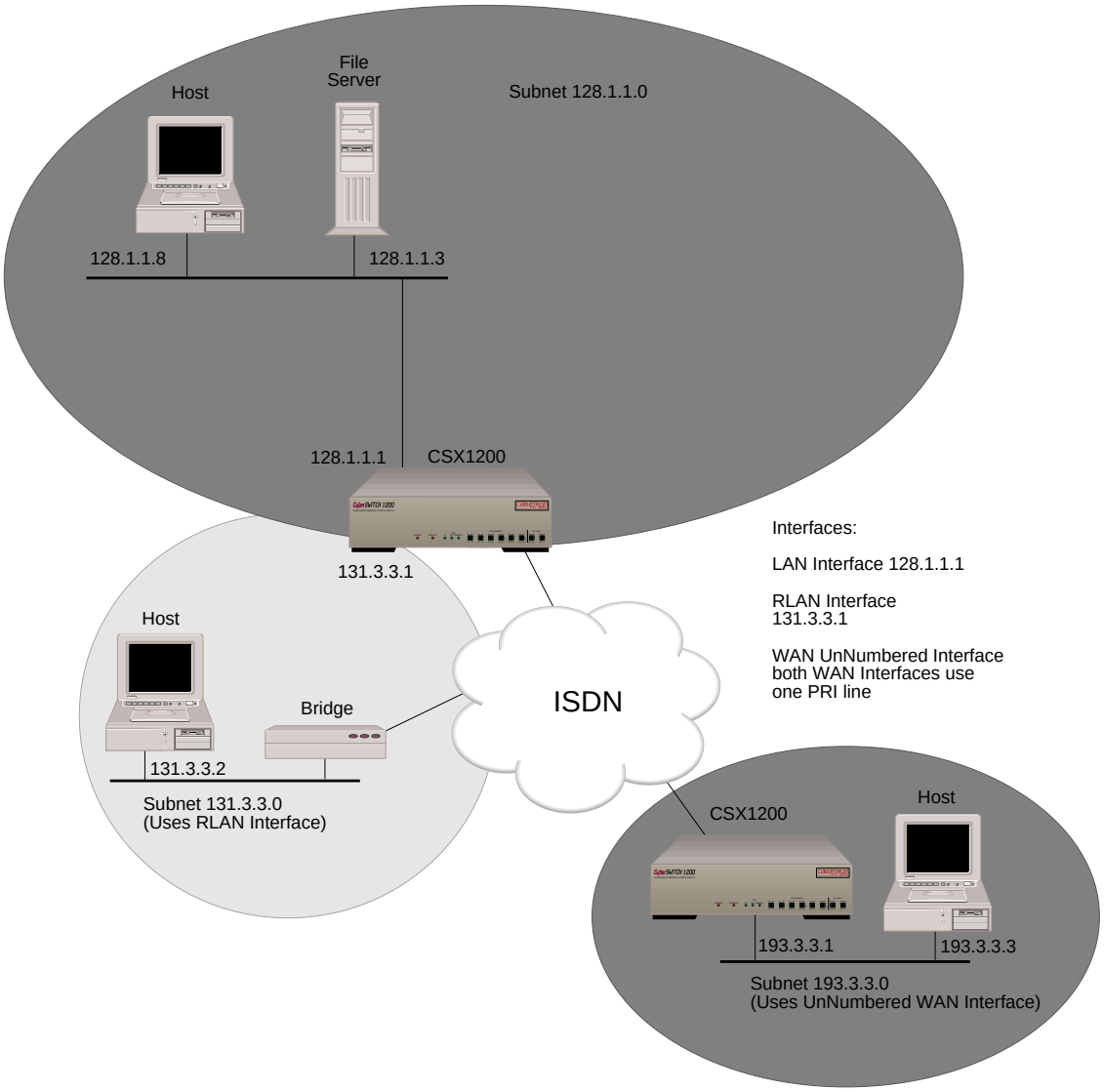
The following diagrams provide examples of each interface type. The variety of network interfaces available allow you to install a wider range of devices at the remote sites.



Example 1: LAN, WAN and WAN Direct Host Interfaces

In *Example 1*, we show three different types of network interfaces and the IP subnets that are used. It should be noted that even though a device only has one physical connection to the WAN, it has more than one logical connection. Also, each one of these logical interfaces can be in different subnetworks.

The LAN interface is the simplest. It specifies the IP address (128.1.1.1) which connects the system to the Ethernet LAN. The Direct Host interface doesn't have an IP address. Devices that use this interface must have an IP address that is on the LAN subnet. The WAN interface in this example is used to connect two IP subnets (128.1.1.0 and 198.1.2.0). A separate subnet (192.2.2.0) is required to connect the subnets. If the remote router supports unnumbered interfaces (as shown in Example 2), then the connecting subnet would not be required.



Example 2: LAN, WAN UnNumbered, WAN Remote LAN Interfaces

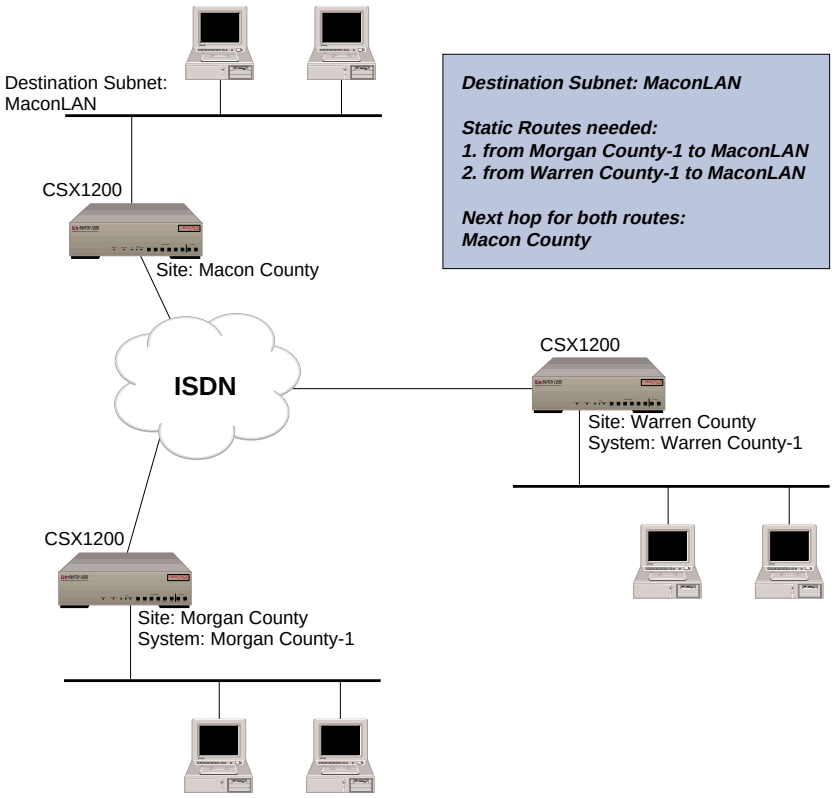
In Example 2, the WAN UnNumbered interface is used to eliminate an unnecessary IP Subnet. The Remote LAN interface is unique in that it extends the IP network over the WAN to remote users which access the network using a bridge device. Thus it makes a simple bridge device appear to be an IP router. This is accomplished by having the system extend its Ethernet to handle the ARPs for the remote bridge.

STATIC ROUTES

You only need to configure static routing entries if you need to access a WAN network that is not directly connected to the system, or if you need to access a LAN network through a router that does not support IP RIP. Static routes specify the IP address of the next hop router or gateway that provides access to this subnet.

When configuring static routes using the IP network *subnet* viewpoint, you are configuring all static routes that *lead* to the subnet. When configuring static routes using the IP network *system* viewpoint, you are configuring all static routes that *begin* at the system.

In the example network shown below, there are two systems (Warren County_1 and Morgan County_1) that need a static route to the subnet MaconLAN. For the *subnet view* there will be two static routes with MaconLAN as the destination, one beginning at Morgan County-1, and one beginning at Warren County-1. For the *system view*, each system will need a static route from the system to the subnet.



CONFIGURING IP NETWORK SUBNET INFORMATION

The use of subnetting provides additional flexibility in addressing. A subnet is a portion of a network that can be considered a single network component.

An IP address that uses subnetting is made up of two types of information: network and host. The network part of the address identifies the segment of the network (the subnet), that the system belongs to. The second part of the address, the host information, uniquely identifies the individual system. For example, if we have a LAN subnet with an IP address of 198.1.1.0, 198.1.1 would be the network number that identifies the subnet. The individual systems on the subnet would also begin the address with 198.1.1, but they would end the address with a unique identifier. For instance, the subnet could have systems with addresses such as 198.1.1.10, 198.1.1.12, where .10 and .12 uniquely identify the systems, and 198.1.1 defines the subnet the systems belong to.

To begin configuring an IP network subnet:

From the menu bar click on *Functions* then click on *IP Network*, then on *Subnets*, or click on the toolbar.

To complete the IP network subnet configuration, you need to configure:

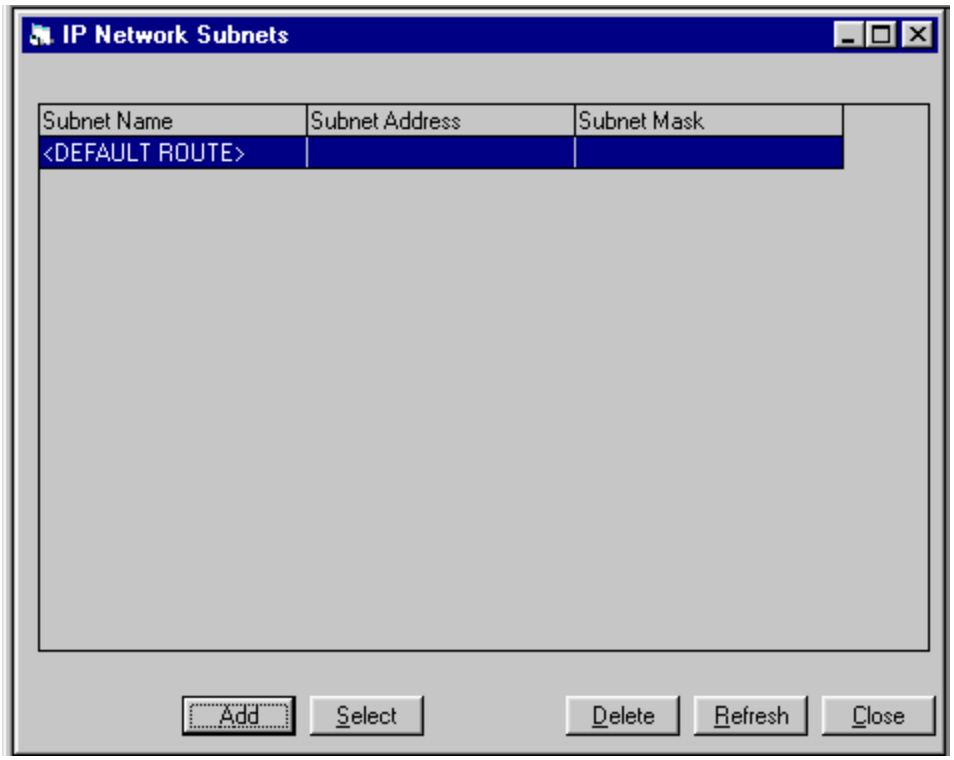
- IP Network Subnet Properties
- IP Network Subnet Interfaces
- IP Network Subnet Static Routes

CONFIGURING IP NETWORK SUBNET PROPERTIES

The first entry in the IP networks subnets table is a special entry with a subnet name of <DEFAULT ROUTE>. This entry is inserted automatically during the SFVRA-CFG installation and cannot be deleted. It does not actually correspond to a real subnet, but by selecting this entry you can edit the default route for systems in your network. All IP packets that do not have an explicit routing table entry will be sent to the default route.

To configure IP network subnet properties:

1. If you are modifying the *default route subnet*:
   From the screen shown below, click on <*DEFAULT ROUTE*>, then click on *Select* (or simply double click on <*DEFAULT ROUTE*>).



You do not need to complete any of the information on the Properties screen for a Default Route. You will only need to enter Static Routes information. Skip ahead to *Configuring Static Routes* for instructions.

2. If you are adding a *nondefault subnet*:
   From the screen shown above, click on *Add*.

3. Complete the *Properties* information.

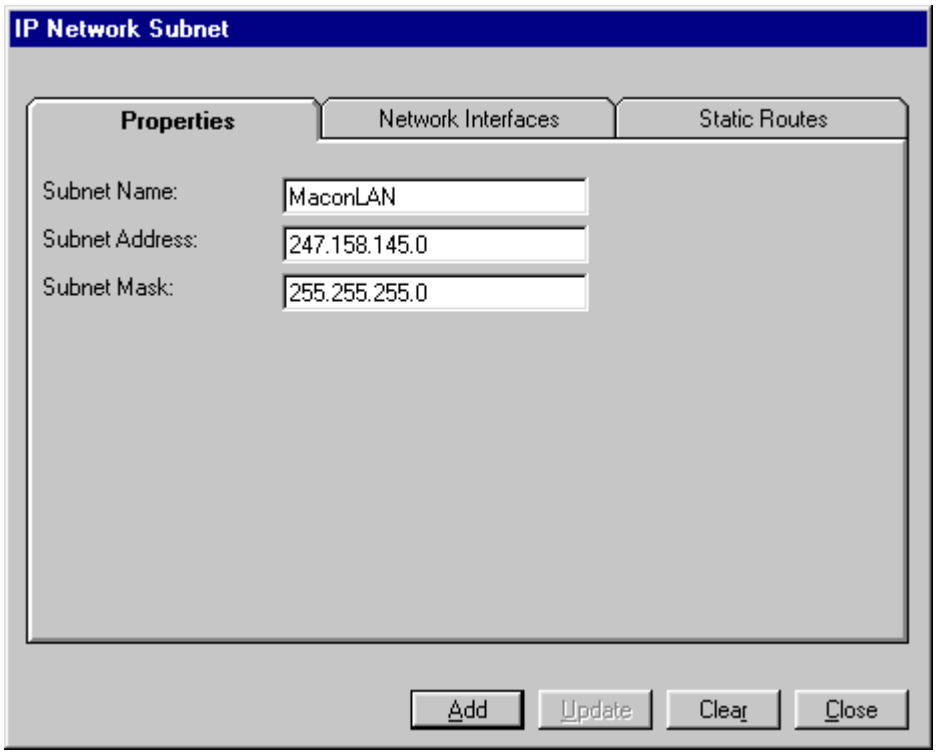
   a. Enter the *Subnet Name*.

      Note If this subnet is the default subnet, the name is preconfigured as <DEFAULT ROUTE>.

   b. Enter the *Subnet Address* (the subnet's IP address). All devices on this subnet must share a portion of the address (this is known as the network number, e.g., the first 24 bits out of 32), and will also have a portion of the address act as a unique identifier (this is known as the host address, e.g, the last 8 bits).

   c. Enter the *Subnet Mask*. The subnet mask is a bit pattern that cancels out unwanted bits so that only the bits of interest are left. For example, if the subnet address is 247.158.145.0, and the mask is 255.255.255.0, the three sets of 255s will cancel out 247.158.145, leaving the last 8 bits as the bits of interest. All devices on the subnet will have an address of 247.158.145.x, where x can be any number from 1 to 254.

After entering information for the above example, the *Properties* screen would appear as:



d. Click on *Add*.

CONFIGURING IP NETWORK SUBNET INTERFACES

Not applicable for Default Routes. To configure *Network Interfaces* information:

1. Click on the *Network Interfaces* tab.
2. Click on *Add*.
3. Configure the IP Network Interface *Properties*.
   a. The Subnet Name is preconfigured.
   b. Select the *Site Name*.
   c. Select the *System ID*.
   d. Select the *Interface Type*. Available types are:
      - LAN
        LAN interfaces define subnet information for an Ethernet port. You must configure a LAN interface for any devices that will communicate over the local network.

- WAN
  WAN interfaces define remote IP devices (hosts or routers) that require access to the central network. This interface represents a different subnet than that connected to a LAN network interface. The WAN interface can be used for both IP Host and PPP remote devices.

- WAN (Remote LAN)
  The Remote LAN interface allows remote MAC layer bridge devices to connect to an IP subnet. All devices connected to the Remote LAN interface are treated as if they were connected to the same Ethernet segment. The system provides an explicit IP router presence on this interface that is implemented over ISDN. IP Address Resolution requests are intelligently propagated to remote bridged networks connected on this interface. The Remote LAN interface can be used for HDLC Bridge and PPP remote devices.

Note: If you define a WAN and a LAN interface to be on the same subnet, the system with the LAN interface will automatically consider WAN devices to be part of the LAN. This will extend the LAN. This special type of interface is called a *Direct Host Interface*.

e. Edit the *Address* field so that it reflects this interface's IP address. Initially, the address field will contain the subnet address. For example, if the subnet's address is 247.158.145.0 (which would initially appear in the address field), and the interface's address is 247.158.145.2, you would only need to change the initial address' 0 to a 2 to reflect the interface's address.

f. Optional: configure the IP Address Pool feature. This feature provides you with a pool of IP addresses that can be dynamically assigned to remote IP devices as they connect to the system. This would occur when a remote IP device calls in to the system and has no IP address, and requests to have one assigned.

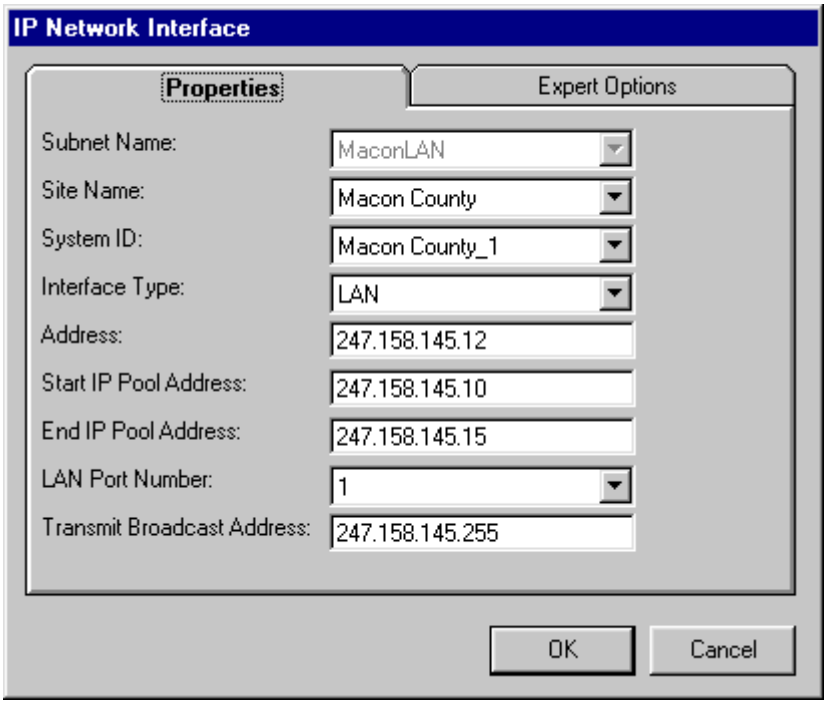
   If this interface makes use of an IP Address Pool:

   - Enter the *Start IP Pool Address*. This is the starting IP address in the range of available IP addresses.

   - Enter the *End IP Pool Address*. This is the ending IP address in the range of available IP addresses.

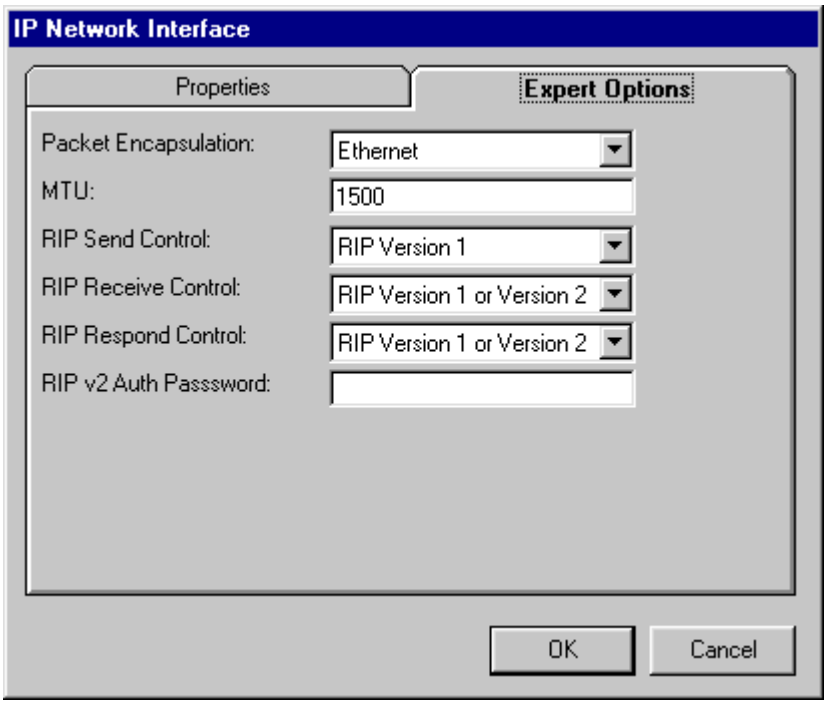
g. For LAN interfaces only. Select the *LAN Port Number* associated with this interface.

h. Enter the *Transmit Broadcast Address*. This specifies the transmit broadcast address on numbered interfaces (meaning all interfaces except interfaces that have been defined as unnumbered). This information is used by all network applications (protocols) that use broadcasting capabilities. In most cases, the default transmit address is used (in example screen below, the default transmit address is 247.158.145.255). A different numerical address would be needed only if the default has been configured, and the machines are not responding to IP RIP or some other broadcast protocol. Regardless of the address entered, the goal is to allow broadcasts from the defined interface to all devices on the local network.



4. Optional: configure *Expert Options*. For most configurations the default values are adequate. To change the default values:

   a. Click on the *Expert Options* tab. A screen similar to the following will be displayed:



Note: The previous screen is associated with LAN or Remote LAN interface types. For WAN interface types, there is no *Packet Encapsulation* field. The WAN interface type also has an additional option for *Host Routes Propagation*.

b. Select the *Packet Encapsulation* type. (For LAN or Remote LAN interface types only.) This specifies the encapsulation type for IP datagrams transferred on this interface. *Ethernet* type encapsulation specifies that IP datagrams are transferred in standard Ethernet frames as specified in RFC-894. *SNAP* type encapsulation specifies that IP datagrams are transferred in 802.3 format frames using the Sub Network Access Protocol (SNAP) as specified in RFC-1042.

c. Enter the *MTU* value. This specifies the maximum number of bytes that can be transmitted on the network interface. Some devices on the network may not be able to receive large data packets. This parameter allows you to maintain compatibility with these devices by setting the MTU to agree with that supported by the device.

d. Select the *RIP Send Control*. This element controls how IP RIP update messages are sent on an IP RIP interface. The following table defines possible choices for IP RIP send control.

Choice	*Meaning*
Do Not Send	No RIP packets are sent.
RIP Version 1	RIP updates compliant with RFC 1058 are sent.
RIP Version 1 Compatibility	RIP Version 2 updates using RFC 1058 route subsumption rules are broadcasted.
RIP Version 2	RIP Version 2 updates compliant with RFC 1723 are multicasted.

Note: RIP Version 1 supports broadcasts.
RIP Version 2 supports multicasts.

e. Select the *RIP Receive Control*. This element controls which version of IP RIP updates are to be accepted. The following table defines possible choices for IP RIP receive control.

Switch	*Meaning*
Do Not Receive	No RIP updates are accepted.
RIP Version 1 Only	Only RIP Version 1 updates compliant with RFC 1058 are accepted.
RIP Version 2 Only	Only RIP Version 2 updates compliant with RFC 1723 are accepted.
RIP Version 1 or Version 2	RIP Version 1 or 2 updates are accepted.

f. Select the *RIP Respond Control*. This element controls how the system responds to IP RIP requests on the interface. The following table defines possible choices for IP RIP respond control.

Switch	*Meaning*
Do Not Respond	No RIP requests are responded to.
RIP Version 1 Only	Responds only to RIP requests compliant with RFC 1058.
RIP Version 2 Only	Responds only to RIP v2 requests compliant with RFC 1723.
RIP Version 1 or Version 2	Responds with the same RIP version format as the version of the request.

g. Enter the *RIP v2 Auth Password*. Used if this interface requires authentication. The authentication password is a user-defined password, 1-16 characters in length. A blank space is not a valid password.

h. Select the *Host Routes Propagation*. (For WAN interfaces only.) This controls how IP RIP packets will be propagated. The default value is Host Routes Propagation disabled (no check mark). With the default, WAN local routes are propagated as subnetwork routes. If Host routes propagation is enabled (with a check mark), host routes will be propagated on other network interfaces only while each remote IP device is connected to the selected system ID.

When the IP RIP host propagation scheme is enabled, it will allow multiple systems on the same LAN to work properly. IP RIP information is then advertised as multiple host routes as they connect to the selected system ID.

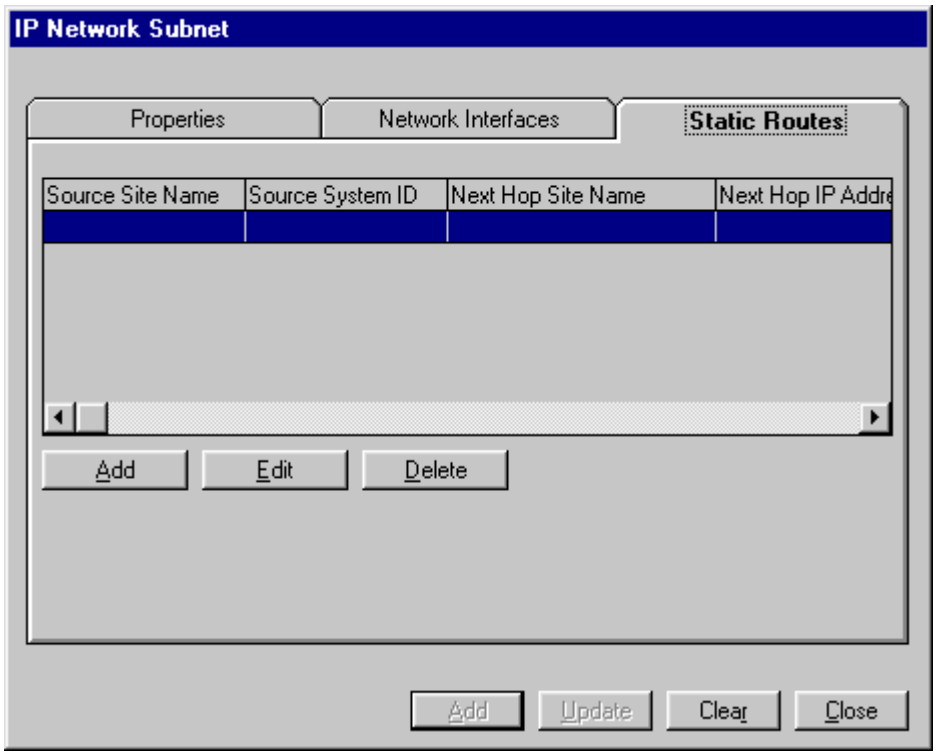
CONFIGURING IP NETWORK SUBNET STATIC ROUTES

You only need to configure static routing entries for systems that need to access a WAN network that is not directly connected to the system, or if the system needs to access a LAN network through a router that does not support IP RIP. Static routes specify the IP address of the next hop router or gateway that provides access to this subnet.

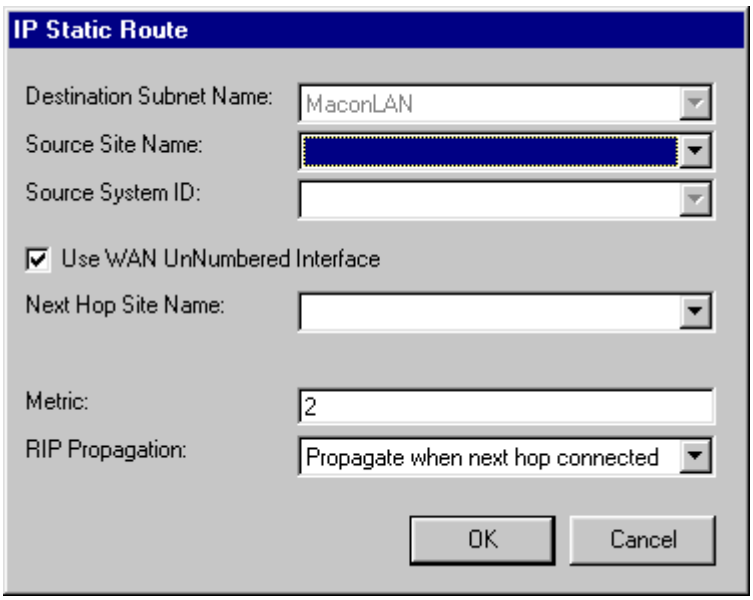
Remember that when configuring static routes through the IP network viewpoint, you are configuring the static routes that *lead* to this subnet.

To configure static routes to a subnet:

1. Click on the *Static Routes* tab. The following screen will be displayed:



2. Click on *Add*. You will see a screen similar to the following:



If you are configuring a default route, the *Destination Subnet Name* will be <*DEFAULT ROUTE*>.

3. Select the *Source Site Name*. This is the starting point of the static route. In other words, this is the site that will be using the static route to connect with the subnet.

4. Select the *Source System ID*. This is the specific system at the source site that will be using the static route to connect with the subnet.

5. If this static route is over a WAN UnNumbered interface:

   a. Make sure a check appears next to *Use WAN UnNumbered Interface*.

   b. Select the *Next Hop Site Name*. This is the device that is the next hop gateway that provides access to the destination subnet.

6. If this static route is over a WAN Numbered interface:

   a. Make sure no check appears next to *Use WAN UnNumbered Interface*.

   b. Enter a *Next Hop Address*. This is an IP address using dotted decimal notation for the next hop gateway that provides access to the destination subnet.

7. Enter the *Metric* value. This is the administrative distance to the destination subnet. The distance is typically measured by the number of hop counts (number of routers) between the source system and the destination subnet, but it is up to you to assign proper value to each route entry. If multiple routes exist to the same destination, the route with the least metric value will be chosen as the primary route. Care must be taken when assigning a metric value of 0, because 0 means the destination is reachable directly and therefore no intermediate router will be used.

8. Select the *RIP Propagation* control. This controls how a static route is propagated via IP RIP. The following table defines possible RIP propagation options.

Flag	*Meaning*
Always Propagate	The route information is always propagated via RIP. Available when the next hop is over a LAN or a WAN interface.
Propagate when next hop connected	The route information is propagated via RIP only when the next hop router is connected to the system. Available when the next hop is over a WAN interface.
Do not Propagate	The static route information is not propagated over the interface. Available only when the next hop is over a LAN or WAN interface.

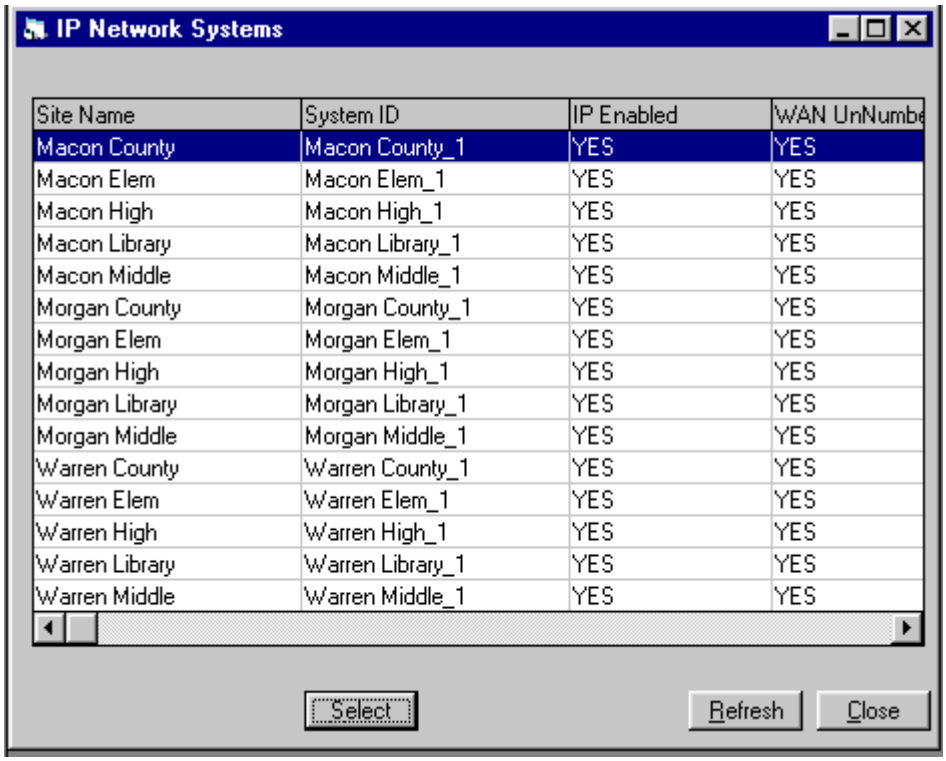
9. Click *OK*. Repeat steps 2 through 8 to add any additional static routes to this subnet.

CONFIGURING IP NETWORK SYSTEMS INFORMATION

The system view looks at IP information with a specific system in mind; you are viewing how the individual system relates to the rest of the network. In this section, we provide instructions for adding a new system to a previously configured subnet.

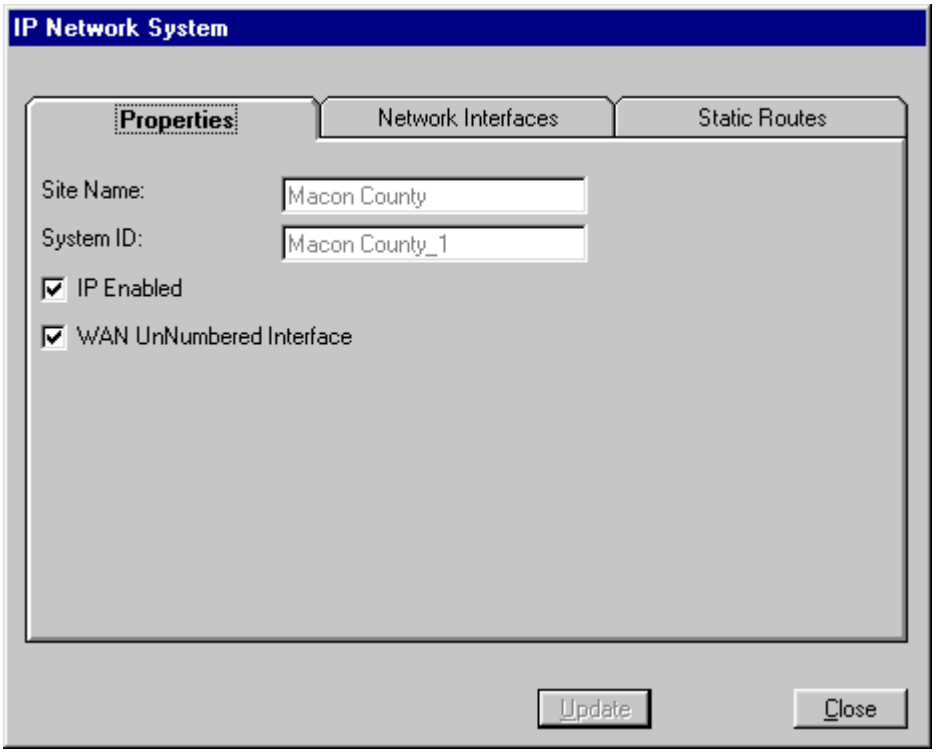
To begin configuring IP network system information:

1. From the menu bar click on *Functions* then click on *IP Network*, then on *Systems*, or click on the toolbar. A screen similar to the following will be displayed:



2. Click on the line entry of the system for which you want to configure IP network information.

3. Click on *Select*. A screen similar to the following will be displayed:



To complete the IP network system configuration, you need to configure:

- IP Network System Properties
- IP Network System Interfaces
- IP Network System Static Routes

CONFIGURING IP NETWORK SYSTEM PROPERTIES

To configure IP network system *Properties*:

1. As the above screen shows, the *Site Name* and *System ID* are preconfigured. These parameter values are taken from site information entered earlier.

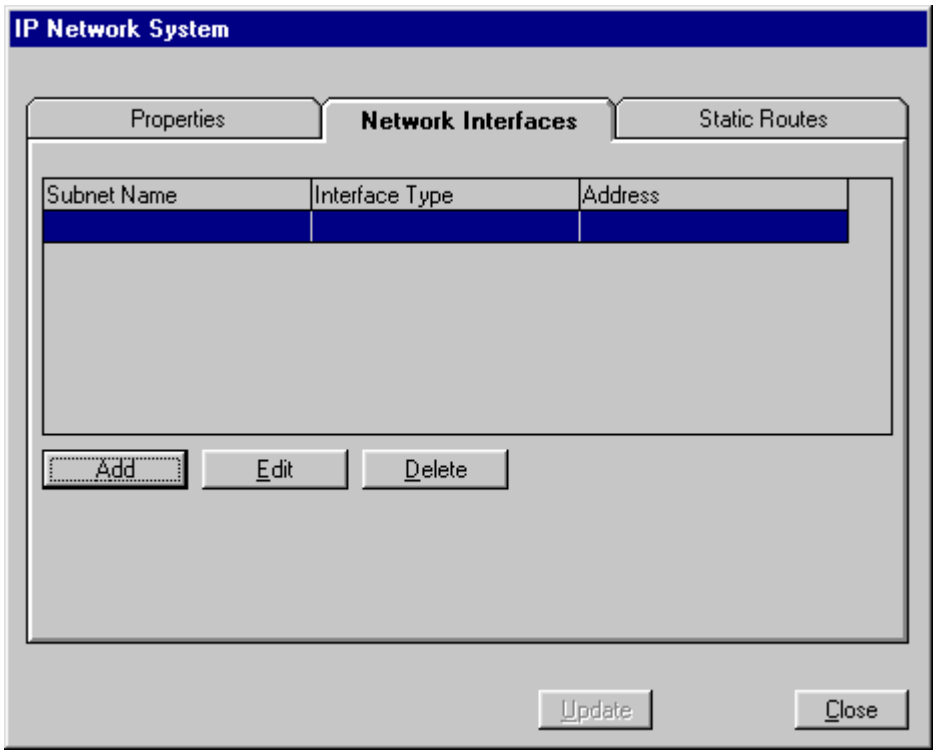
2. You may enable or disable IP routing on a per system basis.

3. You may select to use a *WAN UnNumbered Interface* for this system.

CONFIGURING IP NETWORK SYSTEM INTERFACES

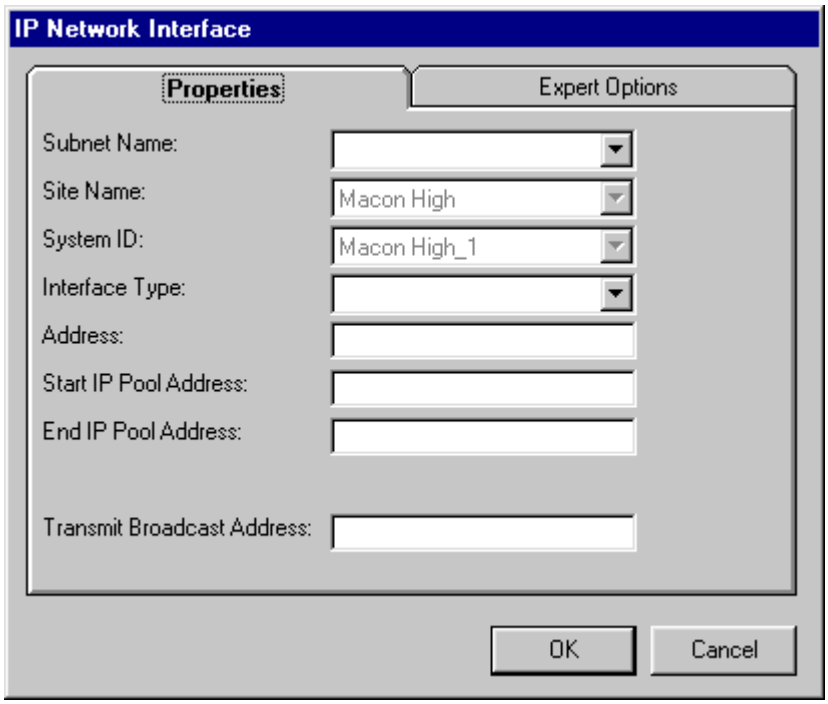
To configure IP network system *Interfaces*:

1. Click on the *Network Interfaces* tab. The following screen will be displayed.



2. Click on *Add*. A screen similar to the following will be displayed.

.



3. Using the above menu, enter the system's IP network interface *Properties*.

   a. Select the *Subnet Name* from the list of previously configured IP subnets.

   b. Select the *Interface Type*. Available types are LAN, WAN, and WAN (Remote LAN). For a definition of each interface type, refer to page 105.

   c. Edit the *Address* field so that it reflects this interface's IP address. Initially, the address field will contain the subnet address. For example, if the subnet's address is 247.158.145.0 (which would initially appear in the address field), and the interface's address is 247.158.145.3, you would only need to change the initial address' 0 to a 3 to reflect the interface's address.

   d. Optional: configure the IP Address Pool feature. This feature provides you with a pool of IP addresses that can be dynamically assigned to remote IP devices as they connect to the system. This would occur when a remote IP device calls in to the system and has no IP address, and requests to have one assigned.

      If this interface makes use of an IP Address Pool:

      - Enter the *Start IP Pool Address*. This is the starting IP address in the range of available IP addresses.

      - Enter the *End IP Pool Address*. This is the ending IP address in the range of available IP addresses.

   e. For LAN interfaces only. Select the *LAN Port Number* associated with this interface.

f. Enter the *Transmit Broadcast Address*. For a definition of transmit broadcast addresses, refer to page 106.

4. Optional: configure *Expert Options*. Note, for most configurations, the default values will be adequate. If you need to configure the expert options for this system, refer to the instructions found under *Configuring IP Network Subnet Interfaces* (the instructions are identical for IP network subnet and system configurations).

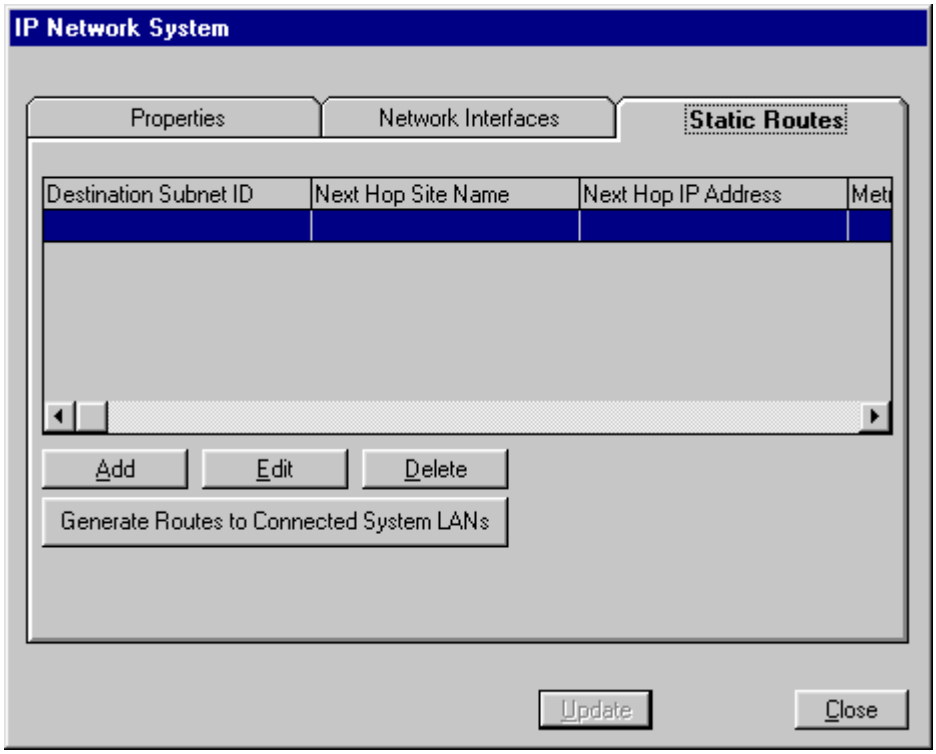
CONFIGURING IP NETWORK SYSTEM STATIC ROUTES

You only need to configure static routing entries for systems that need to access a WAN network that is not directly connected to the system, or if the system needs to access a LAN network through a router that does not support IP RIP. Static routes specify the IP address of the next hop router or gateway that provides access to this subnet.

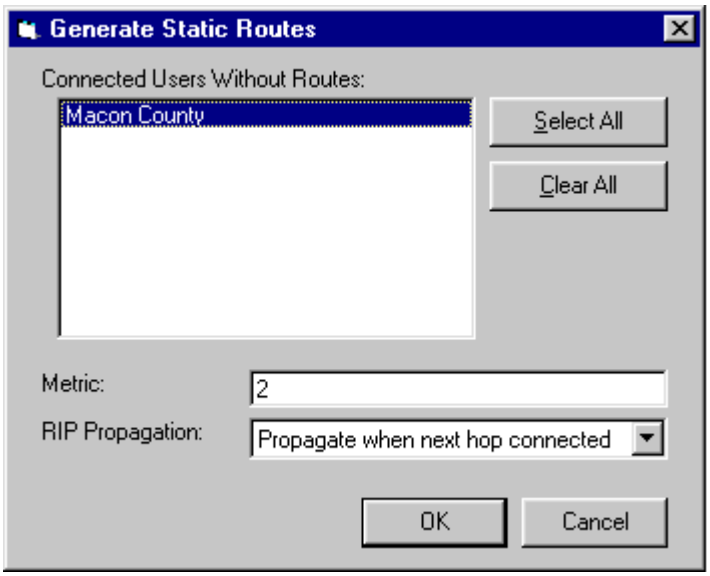
Remember that when configuring static routes through the IP system viewpoint, you are configuring all the static routes that *originate* at this system.

To configure a system's static routes:

1. Click on the *Static Routes* tab. The following screen will be displayed:



2. To configure static routes to sites that have connections with WAN UnNumbered interfaces to this system, click on *Generate Routes to Connected System LANs*. A screen similar to the following will be displayed:



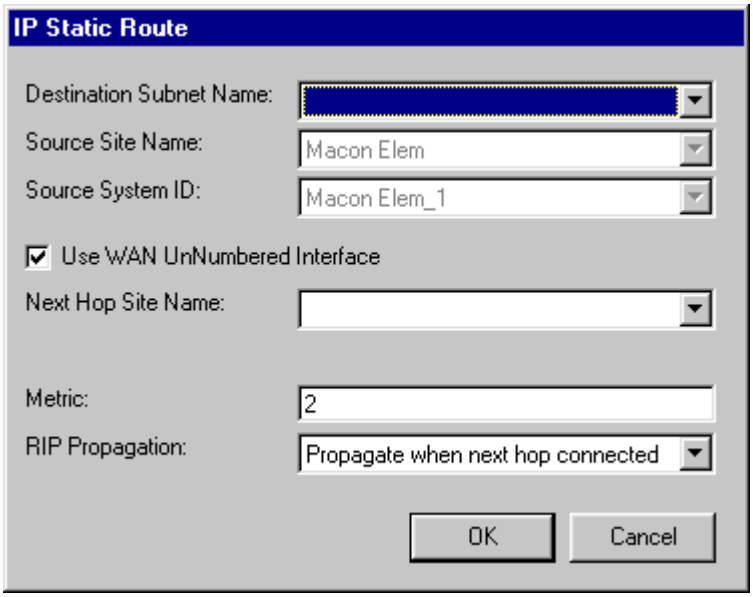
   a. If this screen shows multiple users without routes, select the users you want to establish static routes to by clicking and highlighting the specific names. In the screen above, Macon County is highlighted.

   b. Enter the *Metric* value for the routes. Refer to page 111 for a metric value definition.

   c. Select the *RIP Propagation* control. Refer to page 111 for a RIP propagation control definition.

   d. Click on *OK*.

3. To add any additional static routes, click on *Add*. You will see a screen similar to the following:



4. Select the *Destination Subnet Name* from the list of previously configured subnets. This is the static route's destination subnet. If this will be the site's default route, select <*DEFAULT ROUTE*>.

5. If this static route is over a WAN UnNumbered interface:

   a. Make sure a check appears next to *Use WAN UnNumbered Interface*.

   b. Select the *Next Hop Site Name*. This is the device that is the next hop gateway that provides access to the destination subnet.

6. If this static route is over a WAN Numbered interface:

   a. Make sure no check appears next to *Use WAN UnNumbered Interface*.

   b. Enter a *Next Hop Address*. This is an IP address using dotted decimal notation for the next hop gateway that provides access to the destination subnet.

7. Enter the *Metric* value. Refer to page 111 for a metric value definition.

8. Select the *RIP Propagation* control. Refer to page 111 for a RIP propagation control definition.

9. Click *OK*. Repeat steps 3 through 9 to add any additional static routes for this system.

CONFIGURING IP FILTERS

IP Filters allow you to control the admission and transmission of individual IP datagrams based on the datagram's contents.

As we stated earlier in this chapter, you cannot currently use SFVRA-CFG to configure IP filters. If IP filters are a requirement for your network, there is a way you can configure IP filters by using the system's CFGEDIT configuration utility. You must follow these instructions carefully: do not make any other changes to your system's configuration besides the IP filter configuration. If you make any other changes to the configuration through CFGEDIT, they will be overwritten next time you use SFVA-CFG. The IP filter configuration file is a separate file, and it will not be overwritten.

To configure IP filters using CFGEDIT:

1. At the system prompt, enter the following console command to start-up CFGEDIT:
   `cfgedit`

2. Refer to the Configuring Advanced IP Routing chapter of the Central Site CyberSWITCH User's Guide for instructions for configuring the IP filters.

3. Save your changes and exit CFGEDIT. You will need to restart the system for the changes to take effect.

We must emphasize again that to be able to use SFVRA-CFG again to make configuration changes to your system, *you must not make any other to your system's changes through CFGEDIT except for the IP filter configuration*.

CONFIGURING IPX NETWORK INFORMATION

OVERVIEW

IPX protocol accepts data from remote devices and formats the data for transmission onto the network, and conversely, accepts data from the LAN and formats it so it can be understood by remote devices. In short, IPX allows remote devices and their servers to communicate.

CyberSWITCH systems and 9W006/9W007 SmartSwitch Remote Access Modules support the standard method of routing IPX datagrams over a network. The system provides bandwidth management features to make the interconnection of IPX networks cost effective over demand type connections like ISDN.

You can configure or view IPX network information in one of two ways: at the segment level or at the system level. The segment view looks at IPX network information with the "big picture" in mind; you are viewing how multiple systems interconnect to form an IPX segment. The system view looks at IPX information with a specific system in mind; you are viewing how the individual system relates to the rest of the network.

Depending on which view you will be using to add IPX network information, refer to one of the following two sections for instructions:

- *Configuring IPX Network Segment Information*
- *Configuring IPX Network System Information*

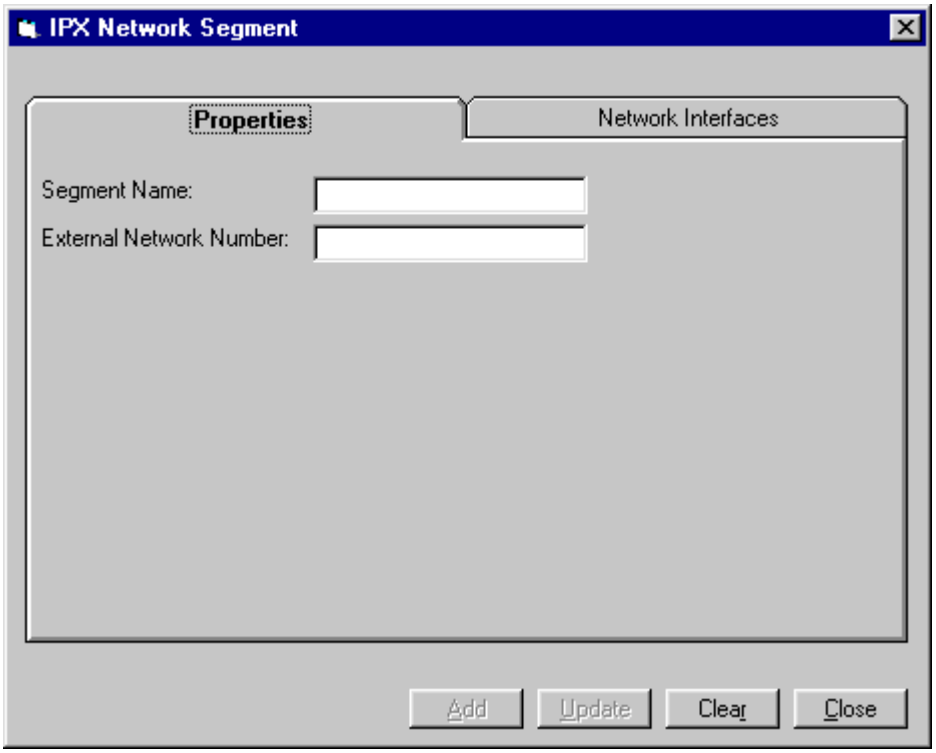
It is important to note that both views share the basic concept of a network interface. *Configuring IP Information* provides a network interface overview.

CONFIGURING IPX NETWORK SEGMENT INFORMATION

The use of segmenting provides additional flexibility in addressing. A segment is a portion of a network that can be considered a single network component.

To begin configuring an IPX network segment:

From the menu bar click on *Functions* then click on *IPX Network*, then on *Segments*, or click on the toolbar. Then click on *Add* to add a new IPX network segment. The following screen will then be displayed:



To complete the IPX network segment configuration, you need to configure:

- IPX Network Segment Properties
- IPX Network Segment Interfaces

CONFIGURING IPX NETWORK SEGMENT PROPERTIES

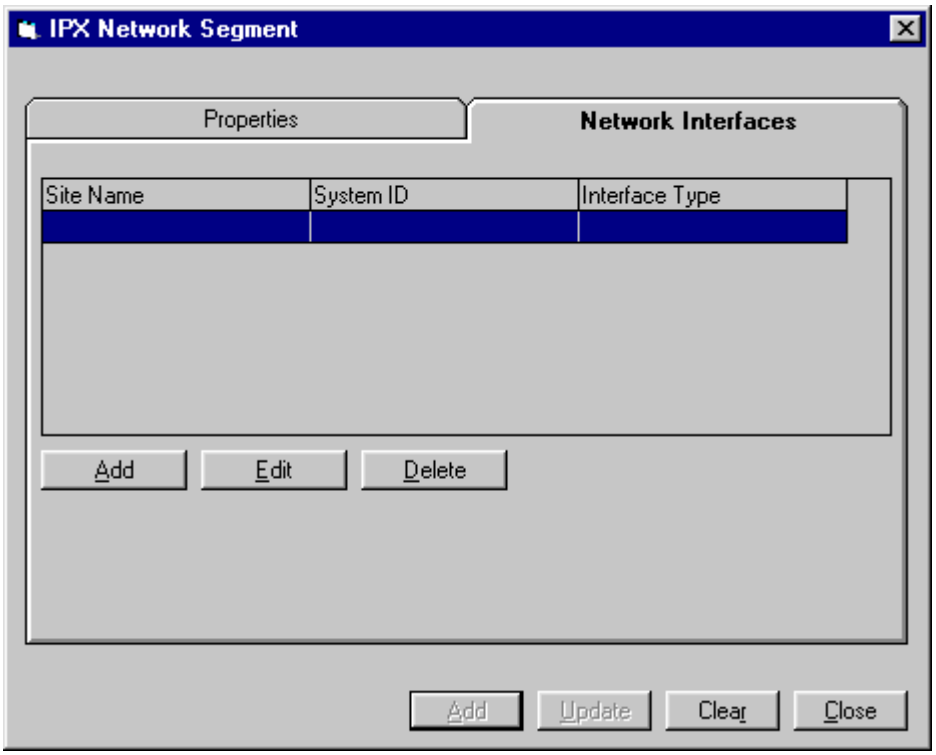
To configure IPX network segment properties:

1. Using the screen shown above, enter a user-defined *Segment Name*.
2. Enter the *External Network Number* for the segment. The external network number is a unique hexadecimal value associated with a network or network cable segment. The value may be from 1 to 8 hexadecimal digits (up to 4 bytes), and is assigned arbitrarily.
3. Click on *Add*.

CONFIGURING IPX NETWORK SEGMENT INTERFACES

To configure IPX network segment interfaces:

1. Click on the *Network Interfaces* tab. The following screen will be displayed:



2. Click on *Add*.

3. Complete the IPX Network Interfaces *Properties.*

   a. The *Segment Name* is preconfigured.

   b. Select the *Site Name.*

   c. Select the *System ID*.

   d. Select the *Interface Type.* Available types are:

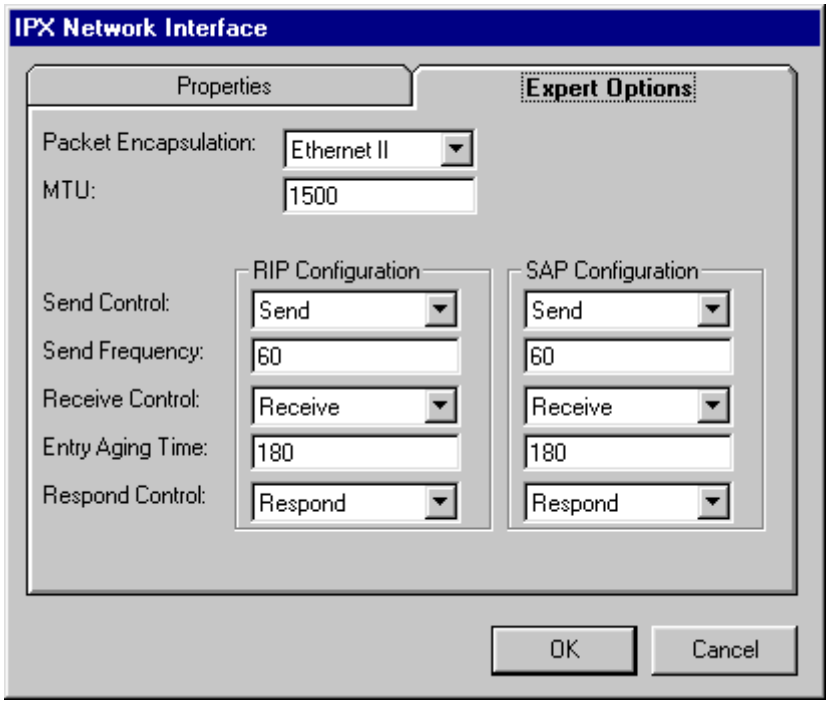
      - *LAN*
        LAN interfaces define segment information for an Ethernet port. You must configure a LAN interface for any devices that will communicate over the local network.

      - *WAN (Remote LAN)*
        The Remote LAN interface allows remote MAC layer bridge devices to connect to an IPX segment. All devices connected to the Remote LAN interface are treated as if they were connected to the same Ethernet segment.

   e. For LAN interfaces only. Select the *LAN Port Number* associated with this interface.

4. Optional: configure *Expert Options*. For most configurations the default values are adequate. To change the default values:

   a. Click on the *Expert Options* tab. A screen similar to the following will be displayed:



   b. Select the *Packet Encapsulation* type. This specifies the encapsulation type for IPX datagrams transferred on this interface. NetWare supports 4 types of encapsulation: Novell SNAP, Novell Ethernet 802.3, Novell Ethernet II, Novell Ethernet 802.2. The Ethernet 802.3 type is the default type for NetWare v2.x and v3.x. The Ethernet 802.2 type is the default type for NetWare v4.x. Choose the appropriate encapsulation type for this network segment.

   c. Enter the *MTU* value. This specifies the maximum number of bytes that can be transmitted on the network interface. Some devices on the network may not be able to receive large data packets. This parameter allows you to maintain compatibility with these devices by setting the MTU to agree with that supported by the device.

   d. Complete the *RIP/SAP Configuration*.

      - Select the *Send Control*. This specifies how RIP / SAP information will be sent on this network interface. When set to *Send*, the system will transmit IPX RIP / SAP packets on this network interface. When set to *Do Not Send*, the system will not transmit any IPX RIP / SAP packets on this network interface.

      - Enter the *Send Frequency Value*. This specifies the frequency at which the system will transmit RIP / SAP packets when the *Send Control* parameter is set to *Send* for this interface. This parameter is a decimal value specified in seconds from 1 to 300. The default value is 60 seconds.

- Select the *Receive Control*. This specifies how the system will process RIP / SAP packets received on this network interface. When set to *Receive*, the system will process IPX RIP / SAP packets received on this network interface and update its internal routing tables. When set to *Do Not Receive*, the system will not process any IPX RIP / SAP packets received on this network interface.

- Enter the *Entry Aging Time*. This specifies the time it takes for the system to age out and make inactive, a dynamic routing table entry learned on this network interface. This parameter is a decimal value specified in seconds from 1 to 180. The default is 180 seconds.

- Select the *Respond Control*. This specifies how the system should respond to RIP / SAP queries from other devices on this network interface. When set to *Respond*, the system will transmit a RIP / SAP response to the requesting device.When set to *Do Not Respond*, the system will ignore RIP / SAP requests received on this network interface.

e. Click on *OK*.

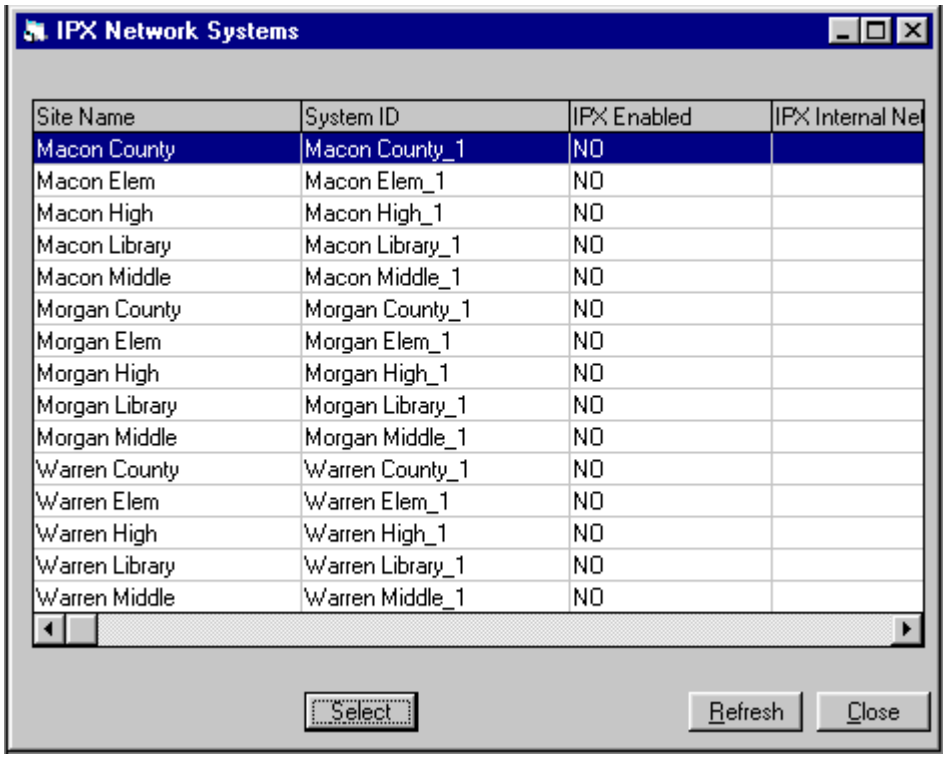
f. Click on *Close*.

CONFIGURING IPX NETWORK SYSTEMS INFORMATION

The system view looks at IPX information with a specific system in mind; you are viewing how the individual system relates to the rest of the network. In this section, we will provide instructions for adding a new system to a previously configured IPX segment.

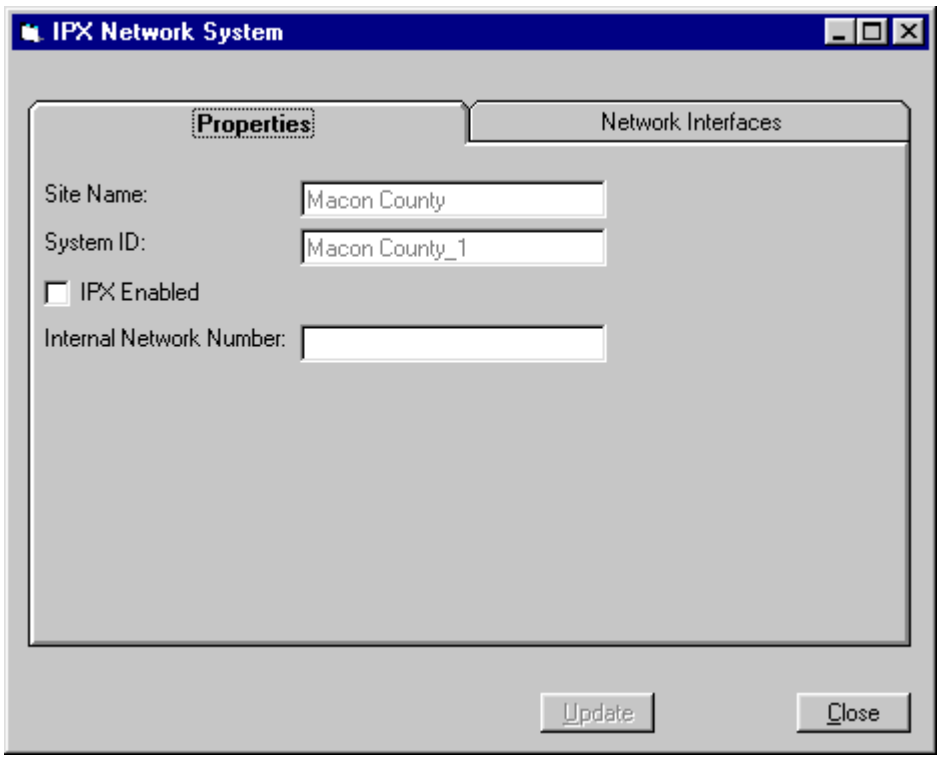
To begin configuring IPX network system information:

1. From the menu bar click on *Functions* then click on *IPX Network*, then on *Systems*, or click on the toolbar. A screen similar to the following will be displayed:



2. Click on the line entry of the system for which you want to configure IPX network information.

3. Click on *Select*. A screen similar to the following will be displayed:



To complete the IPX network system configuration you need to configure:

- IPX Network System Properties
- IPX Network System Interfaces

CONFIGURING IPX NETWORK SYSTEM PROPERTIES

To configure IPX network system *Properties*:

1. As the above screen shows, the Site Name and System ID are preconfigured. These parameter values are taken from site information entered earlier.

2. You may enable or disable IPX routing on a per system basis.

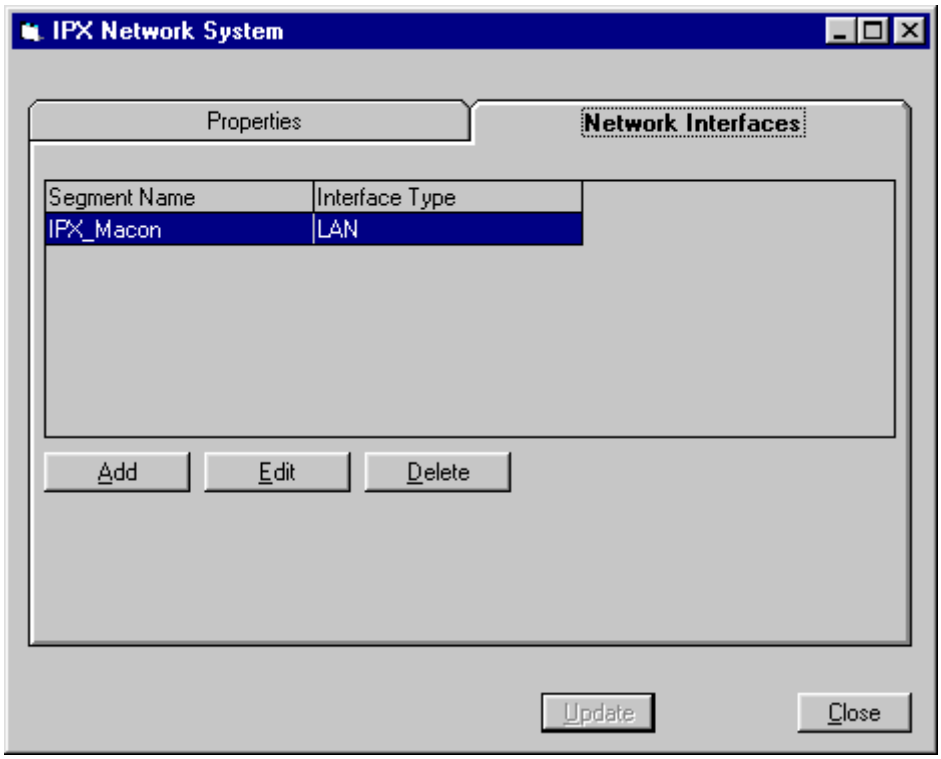
3. Enter the *Internal Network Number*. This number uniquely identifies a specific IPX router in the internetwork. In the Novell environment, an IPX internal network number must be assigned to all IPX routers. This number is an arbitrary value, assigned when the IPX router is configured. It may be 1 to 8 hexadecimal digits in length (up to 4 bytes).

4. Click on *Update*.

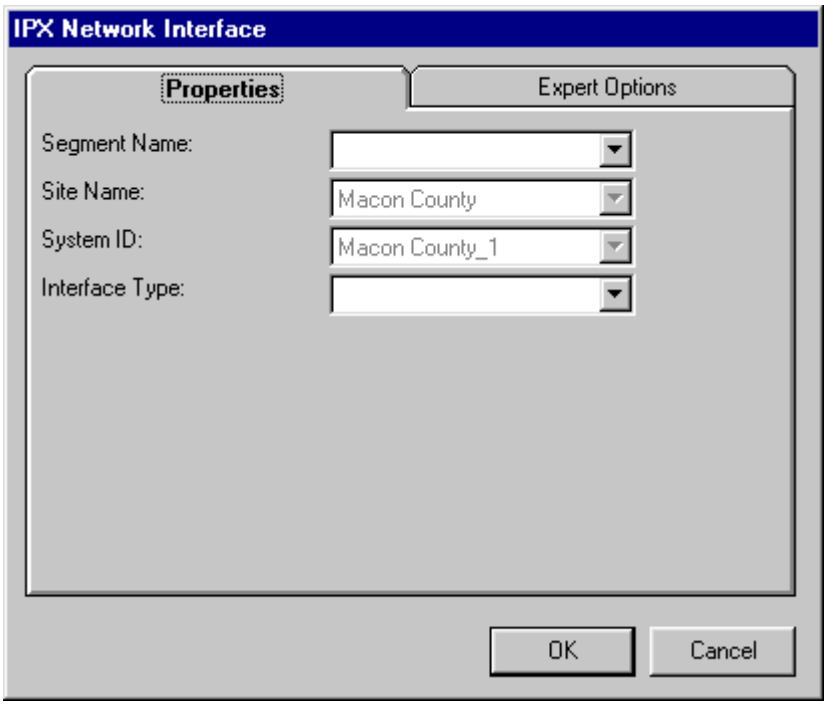
CONFIGURING IPX NETWORK SYSTEM INTERFACES

To configure IPX network system *Interfaces*:

1. Click on the *Network Interfaces* tab. A screen similar to the following will be displayed:



2. Click on *Add*. A screen similar to the following will be displayed:



3. Using the above screen enter the system's IPX network interface *Properties*.

   a. Select the *Segment Name* from the list of previously configured IPX segments.

   b. Select the *Interface Type*. Available types are LAN and WAN (Remote LAN). For a definition of each type, refer to page 122.

   c. For LAN interfaces only. Select the LAN port number associated with this interface.

4. Optional: configure *Expert Options*. For most configurations the default values are adequate. If you need to configure expert options for this system, refer to the instructions found under *Configuring IPX Network Segment Interfaces* (the instructions are identical for IPX network segment and system configurations.)

CONFIGURING APPLETALK NETWORK INFORMATION

OVERVIEW

The AppleTalk routing feature allows CyberSWITCH systems and 9W006/9W007 SmartSwitch Remote Access Modules to efficiently route AppleTalk data as opposed to bridging all data relating to the protocol.

These Cabletron systems support the following AppleTalk protocols:

- Routing Table Maintenance Protocol (RTMP)
- Name Binding Protocol (NBP)
- Zone Information Protocol (ZIP)

Using these protocols, the AppleTalk Routing option allows remote LAN to LAN forwarding of AppleTalk datagrams.

When a datagram is to be forwarded to a remote site, the system will initiate a circuit switched connection and forward the appropriate datagrams to that remote site. As the link utilization increases, the system will make additional connections as required to provide a consistent level of performance to the user. As link utilization decreases, connections will be released.

You can configure or view AppleTalk network information in one of two ways: at the segment level or at the system level. The segment view looks at AppleTalk network information with the "big picture" in mind; you are viewing how multiple systems interconnect to form a segment. Whereas the system view looks at AppleTalk information with a specific system in mind; you are viewing how the individual system relates to the rest of the network.

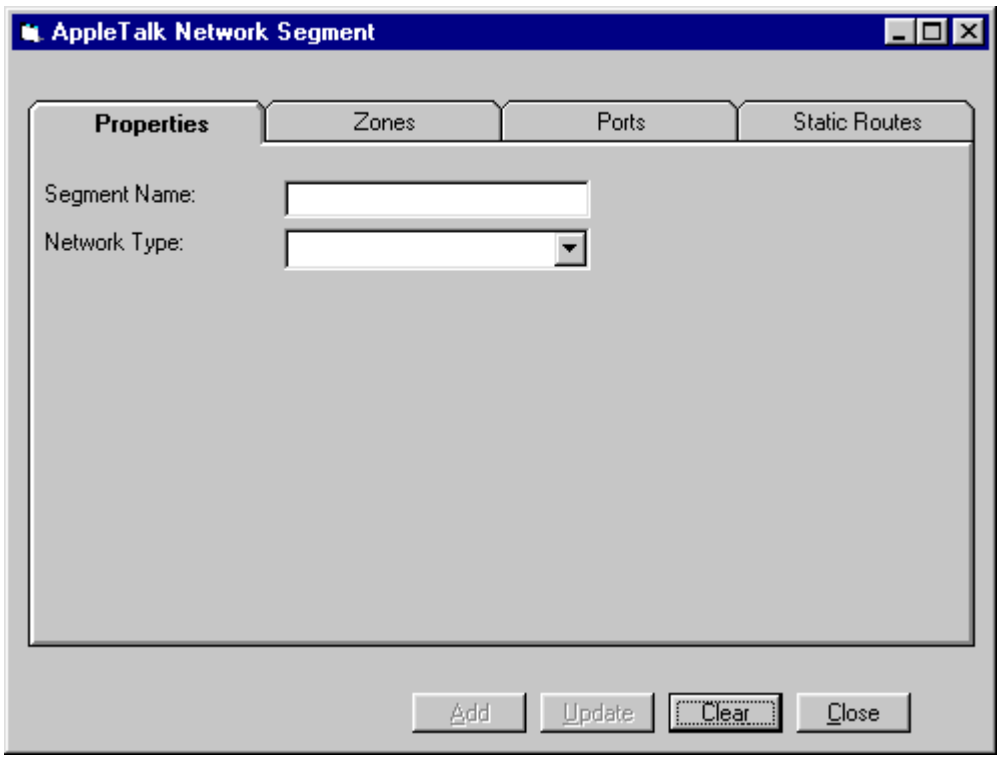
Depending on which view you will be using to add AppleTalk network information, refer to one of the following two sections for instructions:

- *Configuring AppleTalk Network Segment Information*
- *Configuring AppleTalk Network System Information*

CONFIGURING APPLETALK NETWORK SEGMENT INFORMATION

To begin configuring an AppleTalk network segment:

From the menu bar click *Functions* then click *AppleTalk Network*, then on *Segments*, or click on the toolbar. Then click on *Add* to add a new AppleTalk network segment. The following screen will then be displayed:



To complete the AppleTalk network segment configuration, you need to configure:

- AppleTalk Network Segment Properties
- AppleTalk Network Segment Zones
- AppleTalk Network Segment Ports
- AppleTalk Network Segment Static Routes

CONFIGURING APPLETALK NETWORK SEGMENT PROPERTIES

To configure AppleTalk network segment *Properties*:

1. Using the screen shown above, enter a user-defined *Segment Name*.

2. Select a *Network Type*. Possible network types are *Extended* and *NonExtended*.
   The *Extended Network* type indicates that the system is connected to an Extended AppleTalk network, which allows addressing of more than 254 nodes and supports multiple zones.
   The *NonExtended Network* type indicates that the system is connected to a NonExtended AppleTalk network, which supports addressing of up to 254 nodes and supports only one zone.

3. For *Extended Networks*: enter the Start and End Network Number. This is the network number range for the LAN segment. Specifying 0 for both places the segment in discovery mode (a non-seed router), in which the system learns its configuration information from the seed router.

Note that there must be at least one seed router on the network. Discovery mode is not supported for WAN ports, and therefore a valid network range needs to be specified for WAN ports.

4. For *Non-Extended Networks*: enter the Network Number. This is the AppleTalk network number of the LAN segment that the port is connected to. Specifying 0 places the segment in discovery mode (a.k.a., non-seed router), in which the system learns its configuration information from the seed router. Note that there must be at least one seed router on the network. Discovery mode is not supported for WAN ports, and therefore a valid network number needs to be specified for WAN ports.

5. Click on *Add*.

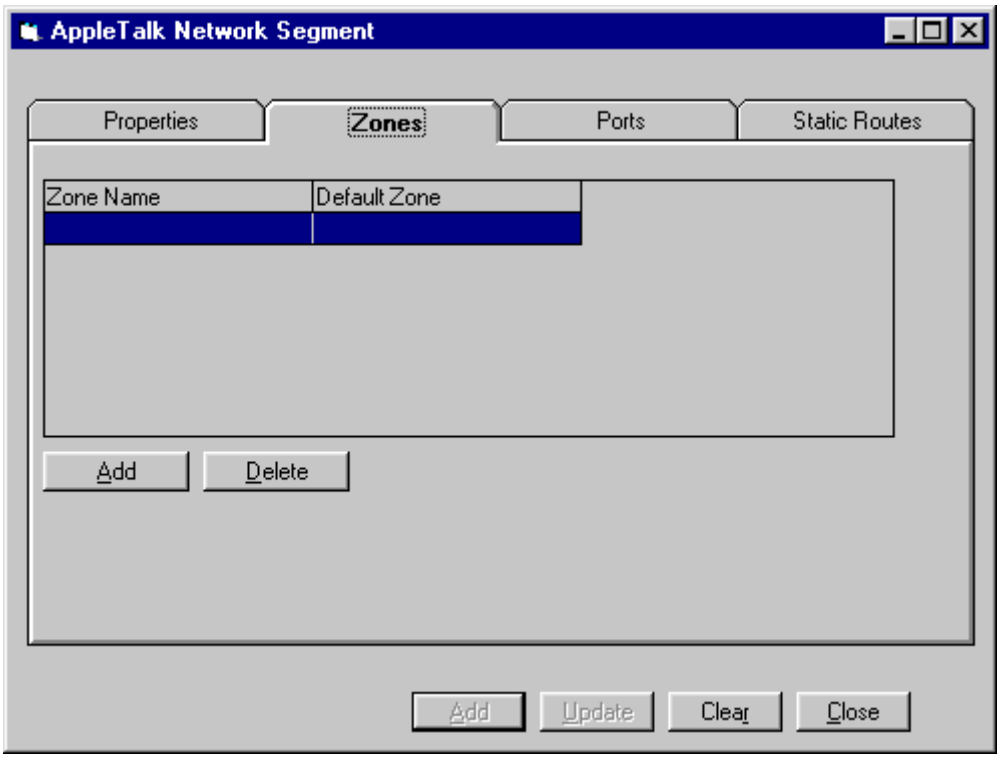
CONFIGURING APPLETALK NETWORK SEGMENT ZONES

Note: Zones should not be configured for segments in the discovery mode.

A zone is a logical group of nodes on an internet, much like the concept of subnetting in the IP world. Within the framework of Phase 2 the logical assignment of zones is limited to 255 zone names for a network. Each name can be configured to represent a logical group within that respective internet. An example would be zone 1 = Marketing, zone 2 = Engineering etc. By configuring an AppleTalk router with logical zones you establish a mode of efficient data transport that acts much the same as IP with multiple subnets.

To configure AppleTalk network segment *Zones*:

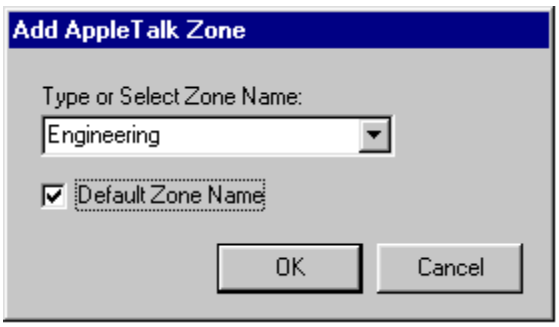
1. Click on the *Zones* tab. The following screen will then be displayed:



2. Click on *Add*.

3. Enter or select a user-defined *Zone Name*.

4. For *extended* network type segments: select whether or not this zone is a default zone. If it is to be the default zone, check the Default Zone Name box as shown below:



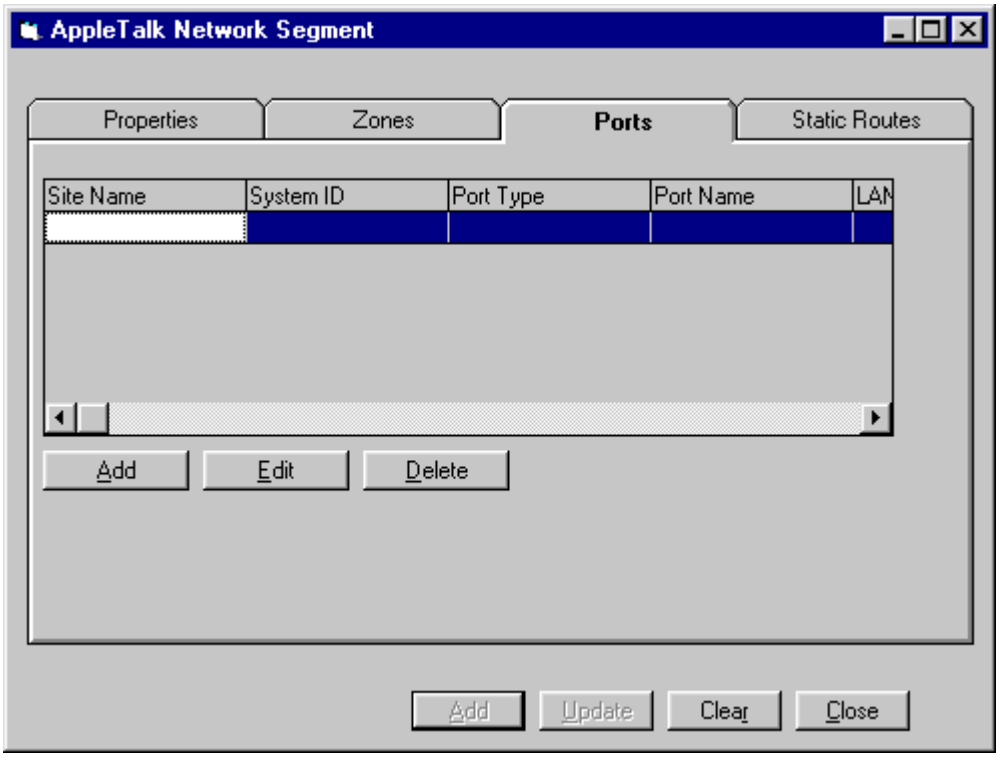
   For ports that are of the Extended network type, you *must* configure a default zone name, then you *may* configure additional zones. For ports that are of the NonExtended network type, you can only configure one zone.

5. Click on *OK*.

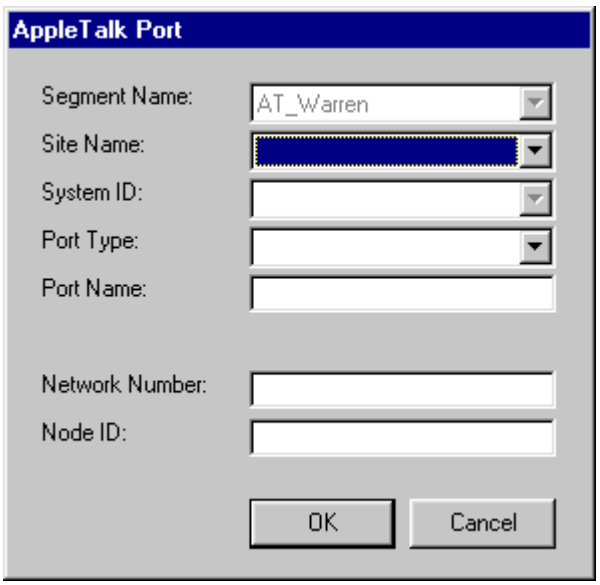
CONFIGURING APPLETALK NETWORK SEGMENT PORTS

To configure AppleTalk network segment *Ports*:

1. Click on the *Ports* tab. The following screen will then be displayed:



2. Click on *Add*. A screen similar to the following will be displayed:



3. Select a *Site Name.*

4. Select a *System ID.*

5. Select a *Port Type*. This is the type of physical network segment that the port connects to. The port type may either be *LAN or WAN*.
   - The *LAN* port type indicates that the system is physically connected to an Ethernet LAN segment.
   - The *WAN* port type creates logical AppleTalk networks over WAN. It creates a logical AppleTalk network that comprises of multiple numbered point-to-point links with the same AppleTalk network range.

6. Enter a user-defined *Port Name* that identifies the port to the system administrator.

   Note: There is an exception to the user-defined port name. If you enter *macdialin* for the port name, this will automatically configure a WAN Mac Dial In port type. This port type allows multiple remote Macintosh devices to connect via numbered point-to-point links.

7. For LAN port types, select the *LAN Port Number*.

8. Enter the port's *Network Number*. This is the AppleTalk network number of the LAN segment that the port is connected to. Specifying 0 places the port in discovery mode (a non-seed router), in which the system learns its configuration information from the seed router. Note that there must be at least one seed router on the network. Discovery mode is not supported for WAN ports, and therefore a valid network number needs to be specified.

9. Enter the port's *Node ID*. If the system is acting as a seed router on this port, then this parameter specifies the suggested AppleTalk Node ID, which is used as the initial value for the AppleTalk address for the port.

10. Click on *OK*.

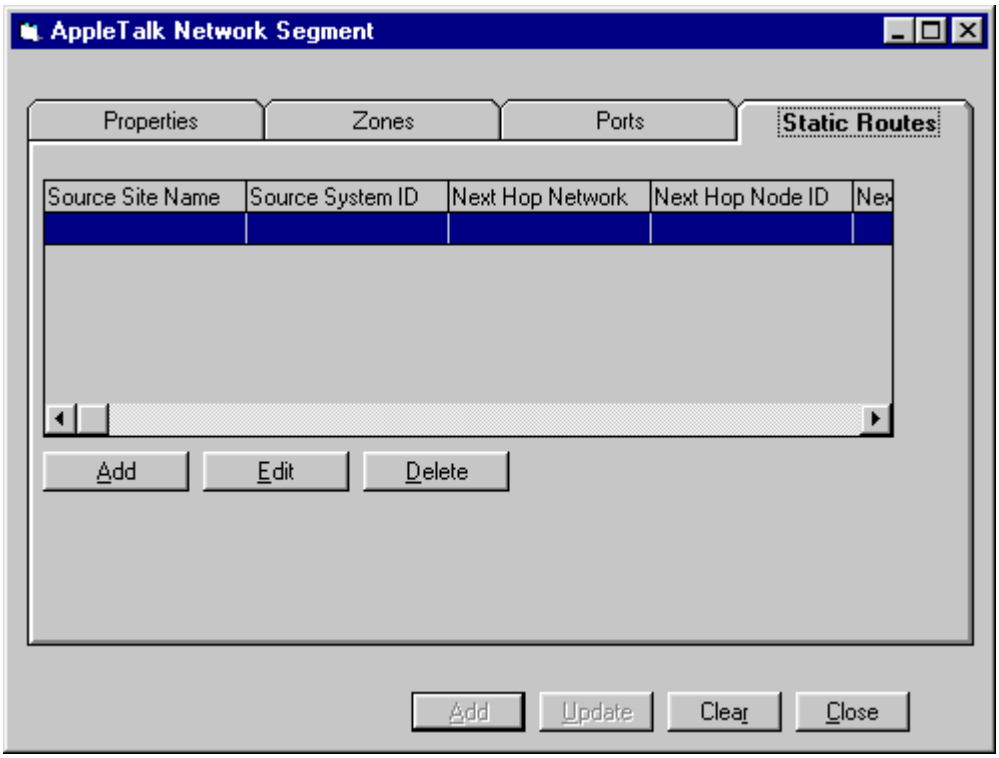
CONFIGURING APPLETALK NETWORK SEGMENT STATIC ROUTES

Note: Static routes should not be configured for segments in the discovery mode.

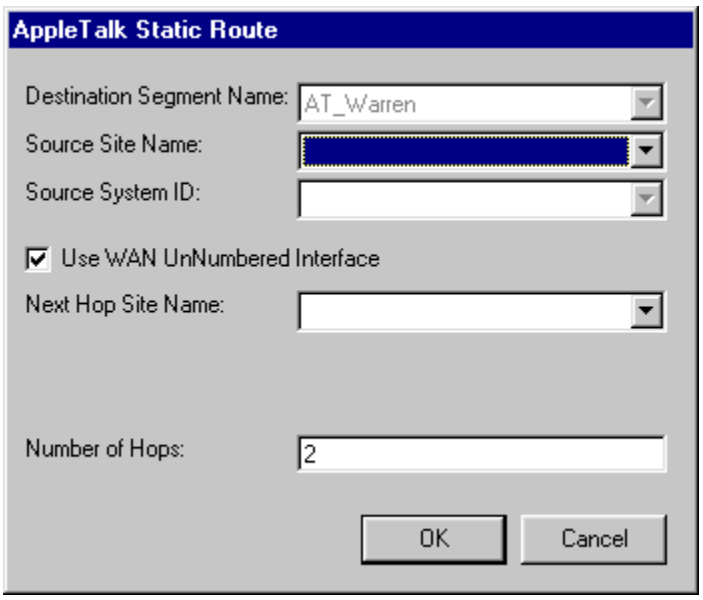
You only need to configure static routing entries if the system needs to access a WAN network that is not directly connected to the system, or if the system needs to access a LAN network through a router that does not support AppleTalk RTMP. Static routes specify the AppleTalk address of the next hop router that provides access to this network.

To configure AppleTalk network segment *Static Routes*:

1. Click on the *Static Routes* tab. The following screen will then be displayed:



2. Click on *Add*. A screen similar to the following will then be displayed:



3. Select the *Source Site Name*. This is the starting point of the static route. In other words, this is the site that will be using the static route to connect with the segment.

4. Select the *Source System ID*. This is the specific system at the source site that will be using the static route to connect with the segment.

5. If this static route is over a WAN UnNumbered interface:

   a. Make sure a check appears next to *Use WAN UnNumbered Interface*.

   b. Select the *Next Hop Site Name*. This is the device that is the next hop gateway that provides access to the destination segment.

6. If this static route is over a WAN Numbered interface:

   a. Make sure a check does not appear next to *Use WAN UnNumbered Interface*.

   b. Enter a *Next Hop Network Number*. This is the network number for the next hop gateway that provides access to the destination segment.

   c. Enter the *Next Hop Node ID*.

7. Enter the *Number of Hops*. This is the administrative distance to the destination segment. The distance is typically measured by the number of hop counts (number of routers) between the source system and the destination segment, but it is up to you to assign proper value to each route entry. If multiple routes exist to the same destination, the route with the least metric value will be chosen as the primary route. Care must be taken when assigning a metric value of 0, because 0 is interpreted as the destination is reachable directly and therefore no intermediate router will be used.

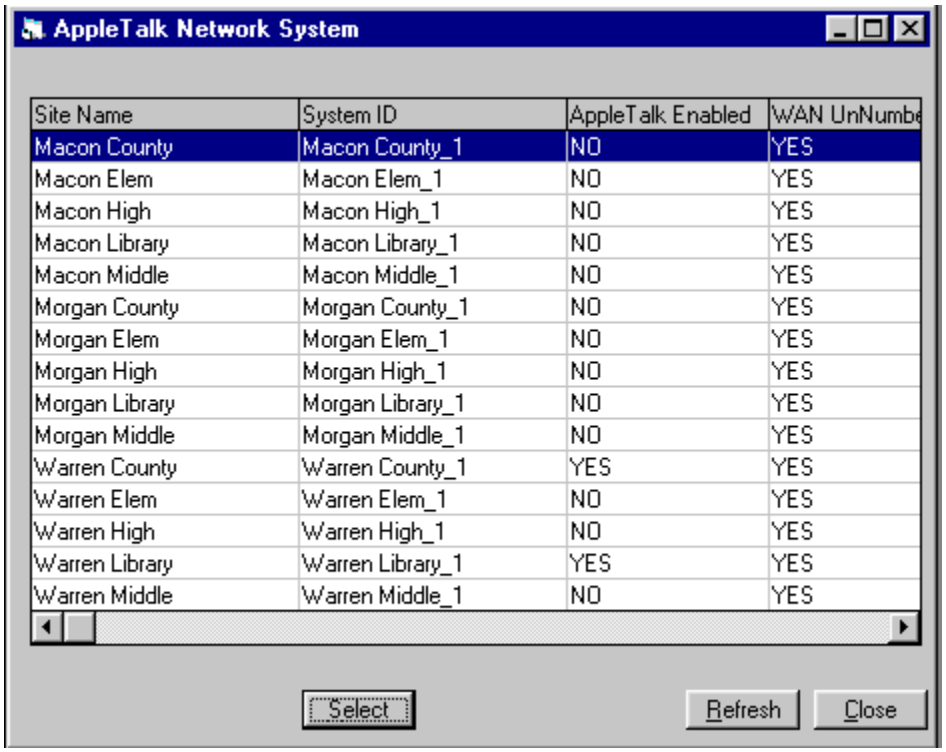
8. Click *OK*. Repeat steps 2 through 7 to add any additional static routes to this segment.

CONFIGURING APPLETALK NETWORK SYSTEM INFORMATION

The system view looks at AppleTalk information with a specific system in mind; you are viewing how the individual system relates to the rest of the network. In this section, we will provide instructions for adding a new system to a previously configured segment.

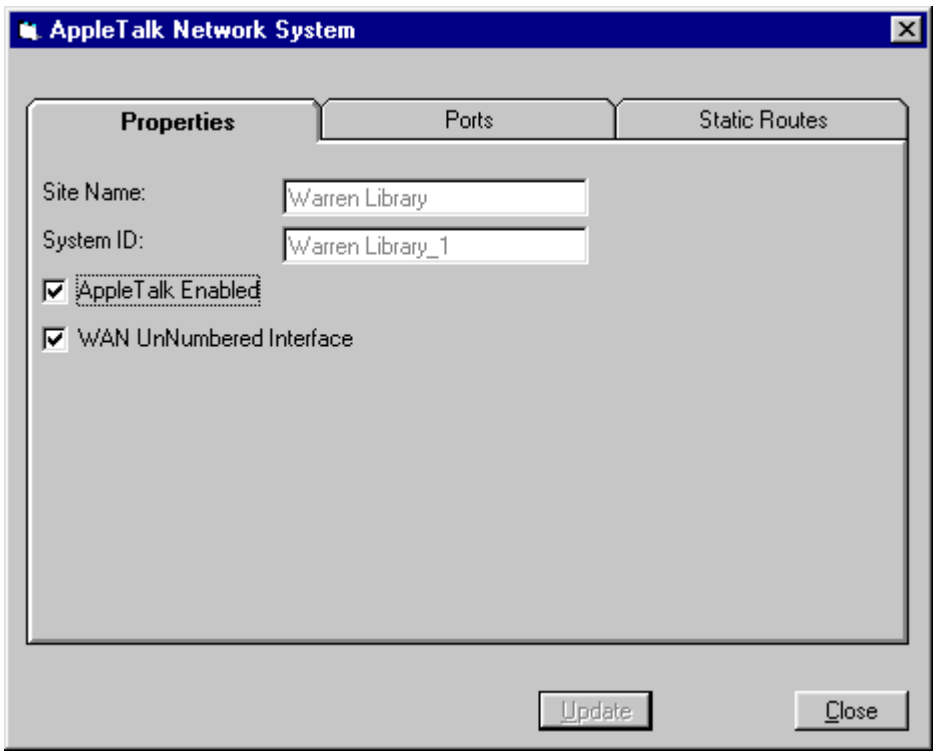
To begin configuring AppleTalk network system information:

1. From the menu bar click on *Functions*, on *AppleTalk Network*, then on *Systems*, or click on the toolbar. A screen similar to the following will be displayed:



2. Click on the line entry of the system for which you want to configure AppleTalk network information.

3. Click on *Select*. A screen similar to the following will be displayed:



4. To complete the AppleTalk network system configuration, you need to configure:

   - AppleTalk Network System Properties
   - AppleTalk Network System Ports
   - AppleTalk Network System Static Routes

CONFIGURING APPLETALK NETWORK SYSTEM PROPERTIES

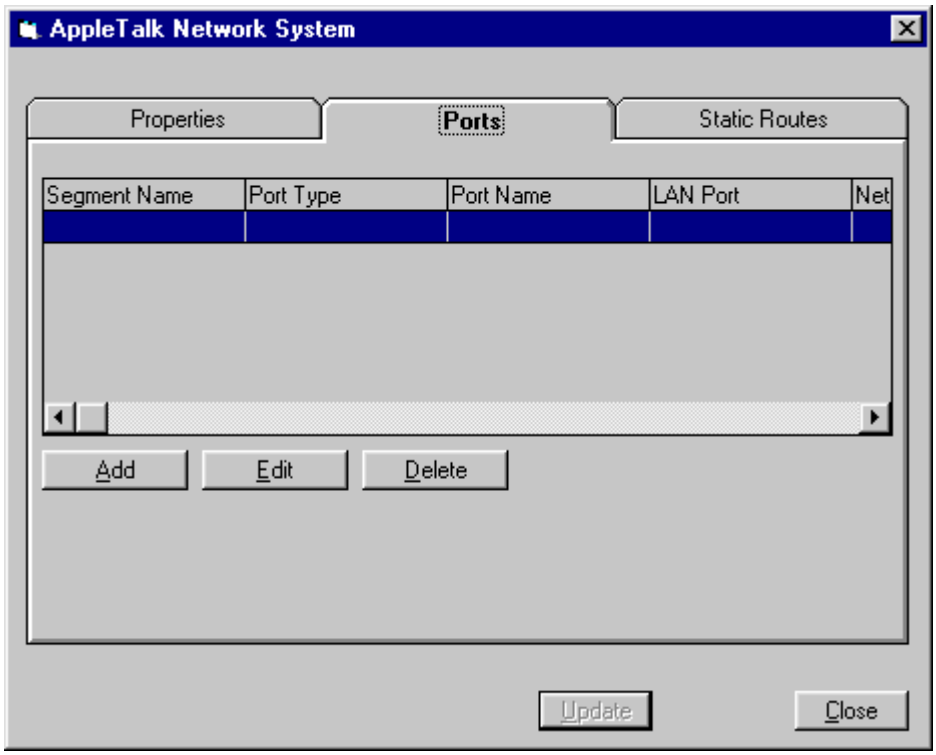
To configure AppleTalk network system *Properties*:

1. As the above screen shows, the *Site Name* and *System ID* are preconfigured. These parameter values are taken from site information entered earlier.
2. You may enable or disable AppleTalk routing on a per system basis.
3. You may select to use a *WAN UnNumbered Interface* for this system.
4. If you have made any changes to the properties, click on *Update*.

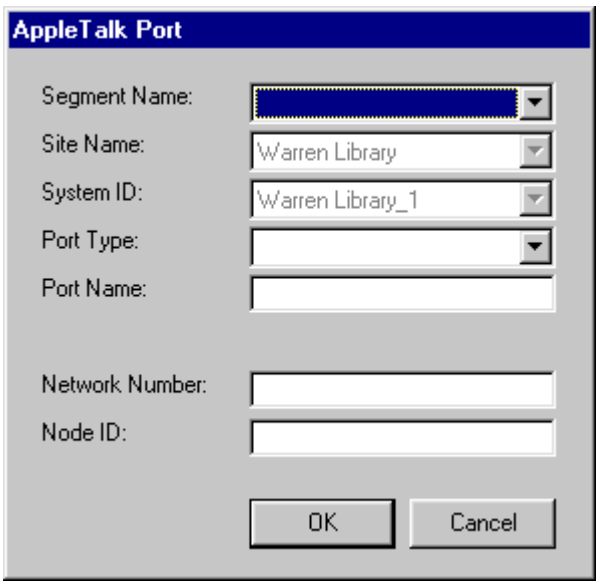
CONFIGURING APPLETALK NETWORK SYSTEM PORTS

To configure AppleTalk network system *Ports*:

1. Click on the *Ports* tab. The following screen will be displayed.



2. Click on *Add*. A screen similar to the following will be displayed:



3. Select the *Segment Name* from the list of previously configured AppleTalk segments.

4. Select the *Port Type*. Available types are LAN or WAN. For a definition of each interface type, refer to page 134.

5. Enter a user-defined *Port Name* that identifies the port to the system administrator.

   Note: There is an exception to the user-defined port name. If you enter *macdialin* for the port name, this will automatically configure a WAN Mac Dial In port type. This port type allows multiple remote Macintosh devices to connect via numbered point-to-point links.

6. For LAN port types, select the *LAN Port Number*.

7. Enter the port's *Network Number*. (For a definition, refer to page 134.)

8. Enter the port's *Node ID*. (For a definition, refer to page 134.)

9. Click on *OK*.

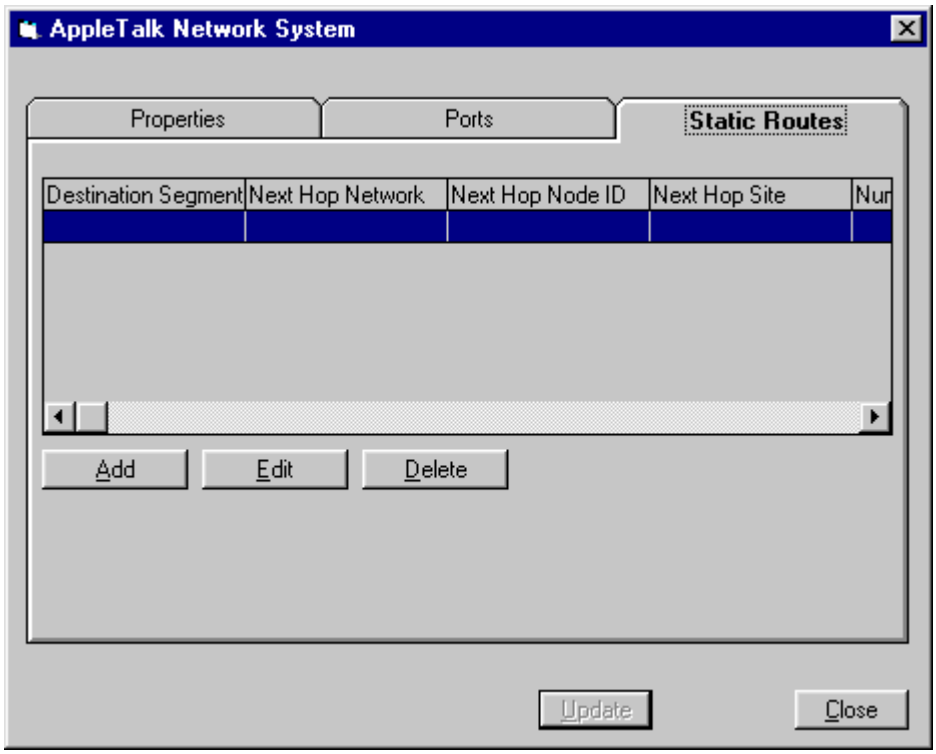
CONFIGURING APPLETALK NETWORK SYSTEM STATIC ROUTES

You only need to configure static routing entries if the system needs to access a WAN network that is not directly connected to the system, or if the system needs to access a LAN network through a router that does not support AppleTalk RTMP. Static routes specify the AppleTalk address of the next hop router that provides access to this network.

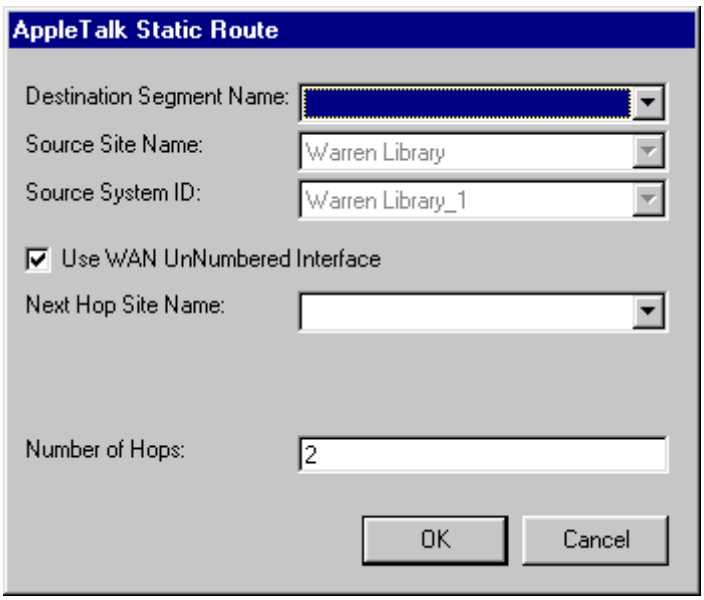
Remember that when configuring static routes through the AppleTalk system viewpoint, you are configuring all the static routes that *originate* at this system.

To configure a system's static routes:

1. Click on the *Static Routes* tab. The following screen will be displayed:



2. Click on *Add*. You will see a screen similar to the following:



3. Select the *Destination Segment Name* from the list of previously configured segments. This is the static route's destination segment.

4. If this static route is over a WAN UnNumbered interface:

   a. Make sure a check appears next to *Use WAN UnNumbered Interface*.

   b. Select the *Next Hop Site Name*. This is the device that is the next hop gateway that provides access to the destination segment.

5. If this static route is over a WAN Numbered interface:

   a. Make sure no check appears next to *Use WAN UnNumbered Interface*.

   b. Enter a *Next Hop Network Number*. This is the network number for the next hop gateway that provides access to the destination segment.

   c. Enter the *Next Hop Node ID*.

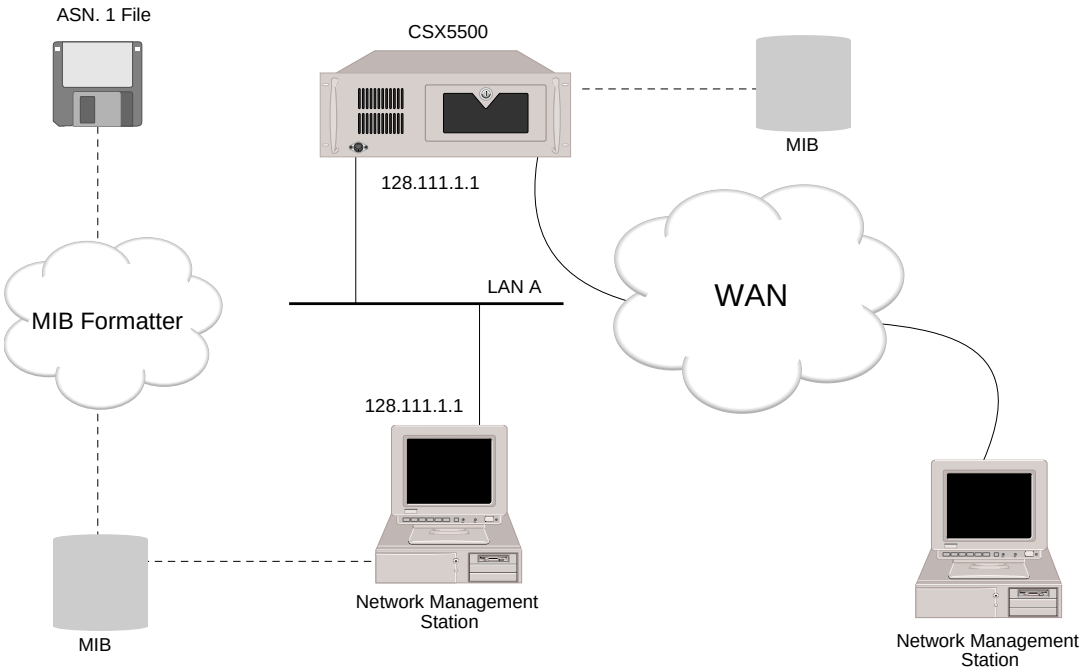
6. Enter the *Number of Hops*. (For a definition, refer to page 136).

7. Click *OK*. Repeat steps 2 through 6 to add any additional static routes for this system.

CONFIGURING SNMP MANAGEMENT GROUPS

OVERVIEW

When SNMP is employed to manage CyberSWITCH systems or 9W006/9W007 SmartSwitch Remote Access Modules, the systems (or modules) become SNMP Agents. Being an SNMP Agent allows the system to be monitored from a local and/or a remote Network Management Station (NMS) via the Simple Network Management Protocol. The User Datagram Protocol (UDP) and the Internet Protocol (IP) are used by the SNMP Agent to provide the transport datagram service needed to exchange SNMP messages. Thus only those systems that have enabled the IP routing operating mode can make use of SNMP.

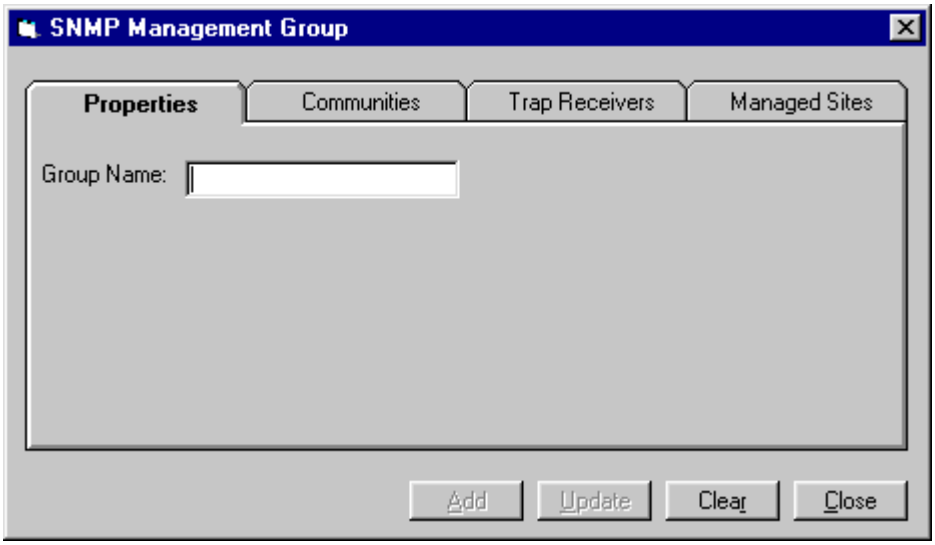


The SNMP Agent will process all SNMP Protocol Data Units (PDUs) which are received at a LAN or a WAN port. This is shown in the above illustration, which depicts a network in which the Network Management Station on LAN A or the remote NMS can manage the systems.

The SFVRA-CFG allows you to form SNMP Management Groups. SNMP Management Groups are a selected group of sites that are collectively managed by an SNMP Manager.

To begin configuring SNMP Management Groups:

From the menu bar click on *Functions* then click on *SNMP*, or click on the toolbar. Then click on *Add*. The following screen will then be displayed:



Use this resulting screen and the following sections to complete the SNMP Management Group configuration.

CONFIGURING SNMP MANAGEMENT GROUP PROPERTIES

1. Using the above *Properties* window, enter a user-defined *Group Name* for the SNMP Management Group you are configuring.

2. Click on *Add*.

CONFIGURING SNMP MANAGEMENT GROUP COMMUNITIES

SNMP Community Names identify the community to which an SNMP Manager, along with the Agent(s) that it manages, belongs. It is used to authenticate an SNMP PDU. *"public"* is a widely used Community Name. These SNMP *Communities* are supported by devices at the sites included in this SNMP Management Group. To configure Communities:

1. Click on the *Communities* tab.

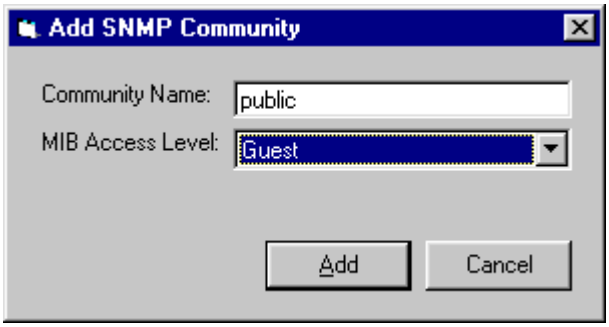
2. Click on *Add*.

3. Enter a user-defined *Community Name*. This name will be associated with a defined MIB Access Level.

4. Select the *MIB Access Level* associated with the Community Name. It dictates the level of access available to the associated Community Name. The following is a chart of the three possible access levels and their access privileges.

Access Level	*Access Privileges*
Guest	get (read) MIB-II system group only
User	get (read) all MIB-II and Enterprise MIB objects
Admin	get (read) all MIB objects and set (write) all MIB objects whose access field is defined to be read-write

As shown below, we have configured public as the Community Name, with guest privileges.



5. Click on *Add*.

DESIGNATING SNMP MANAGEMENT GROUP TRAP RECEIVERS

A *Trap* is a special unsolicited PDU that an SNMP Agent will generate when it detects a pre-specified condition, such as ColdStart, LinkDown, or AuthenticationFailure. Traps are used to monitor the network's state. The *Trap Receiver* is a device designated to receive the SNMP Agent's (a CyberSWITCH's or Remote Access Module's) Trap PDUs. To designate the Trap Receivers that will receive the Trap PDUs generated by the SNMP Management Group's sites:

1. Click on the *Trap Receivers* tab.

2. Click on *Add*.

3. Enter the *IP Address* of the device acting as the Trap Receiver.

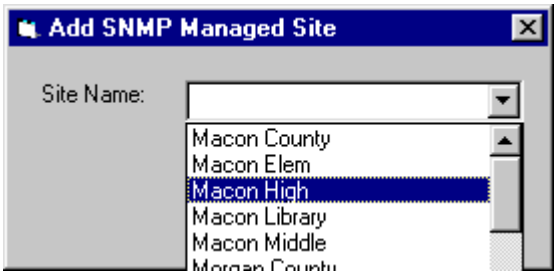
4. Select the *Community Name* associated with the device acting as the Trap Receiver.

5. Click on *Add*.

SELECTING SNMP MANAGEMENT GROUP MANAGED SITES

To designate which sites to include in this SNMP Management Group:

1. Click on the *Managed Sites* tab.
2. Click on *Add*.
3. Select a Site Name from the displayed list as shown below:



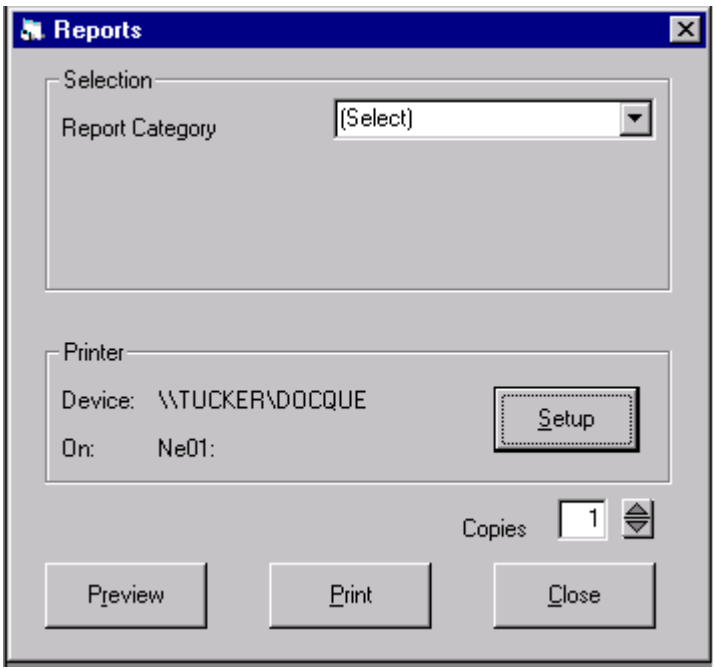
4. Click on *Add*. Note that the site SNMP settings are derived from the site template associated with the site.
5. Repeat steps 3 and 4 for each site you wish to add to this group.
6. Click on *Close*.

SFVRA-CFG REPORTS

You can generate reports that summarize the information you have configured using SFVRA-CFG. You may select a report category and then narrow down the information included in report. For example, you may select IP Subnet as the report category, then you can select a specific connection group and a specific IP Subnet.

To run a report:

1. Click on *Functions* then click on *Reports*. You will see a window similar to the following:



2. Select a *Report Category*.

3. Make a selection from the available options for that particular report category.

4. If you will be printing out the report, check to see that the *Printer* configuration is correct. Click *Setup* and make any changes if necessary.

5. Select to either *Preview* or *Print* the report.

EXPORTING CONFIGURATION FILES

OVERVIEW

You can use the SFVRA-CFG to configure a network centrally. To do this, you would first enter configuration data for each system, generate each system's configuration files separately (with the system's view of the network), then download the files to the systems electronically.

The SFVRA-CFG is also a convenient way to make intermittent updates to established networks. For example, if a card was added to a PC-based CyberSWITCH, you could change that system's configuration to include the new option card. You would then generate new configuration files for that system, then transfer the new files to the system. It is important to note that downloading these configuration files does not update the system's existing configuration files, it overwrites them.

If you are generating and downloading configuration files updates for a system that uses an SFVRA database for user information, you will have to generate and update configuration files for the system *and* for its SFVRA database. If you are generating and downloading configuration files updates for a system that uses a local user database, you only need to generate and update system configuration files for the system.

In *System Configuration Files*, we provide instructions for generating, downloading, and copying system files. In *SFVRA Database Data*, we provide instructions for generating, downloading, and resetting SFVRA database data.

SYSTEM CONFIGURATION FILES

Generating, downloading, and copying system configuration files is done from the SFVRA-CFG's Export Configuration Menu. To get to that menu:

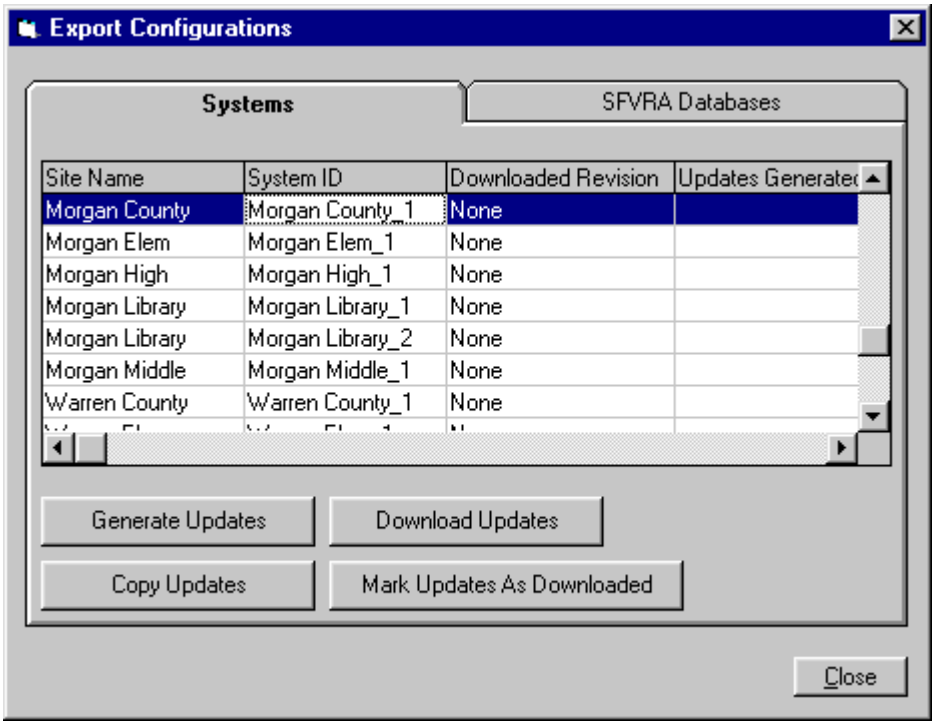
From the menu bar, click on *Options*, then click on *Export Configurations*, or simply click on the toolbar.

Instructions for generating, dowloading, and copying updated system configuration files are described in the following sections.

GENERATING CONFIGURATION UPDATES

To generate an update of a system's configuration files:

1. Click on the *System ID* of choice. In the screen shown below, system Morgan County_1 of site Morgan County has been selected.



   You can also highlight multiple system IDs. This will allow you to concurrently generate updates for multiple systems. Note that you can only download or copy updates one at a time.

2. Click on *Generate Updates*.

3. You should see a message stating that the update for the system has generated successfully. If the message includes warnings, correct any errors described in the warnings.

4. Click on *Close*. Note that the Updates Generated field displays *YES* (it was previously blank). This indicates that the updated configuration files are ready for downloading.

After the configuration updates have been generated, you can choose to either *download* the updates directly to the system, or *copy* the updates to a defined destination such as a diskette. The sections below provide instructions for downloading and copying configuration updates.

DOWNLOADING CONFIGURATION UPDATES

Note: Downloading updated configuration files does not update the system's existing configuration files, it overwrites them.

To download a system's updated configuration files:

1. From the Systems Menu, click on *Download Updates*.

2. You will see a dialog box with the system's IP address. The SFVRA-CFG downloads the configuration files to this address. The SFVRA-CFG retrieves the system's IP address from previously configured data. The SFVRA-CFG retrieves the IP address as follows:
   - If you configured a LAN interface for the system, it will retrieve the IP address you configured for that interface.
   - If there is no LAN interface configured, it will check to see if you configured a WAN numbered interface. If so, it will use that address for the system's IP address.
   - If you are configuring new systems centrally with plans to move the systems to their site after they are completely configured, refer to *New Network Configuration*.

3. Select which revision to download. Choices are:
   a. *Downloaded Revision*
      This choice will be available if you have already downloaded a configuration update directly to the system.
   b. *New Revision*
      This choice will be available if you have generated updates, but have not downloaded them yet.

4. Click on *OK*.

5. You should see a message reporting that your download was successful. If the message includes warnings, correct any errors described in the warnings.

6. Click on *Close*.

7. The *Updates Generated* field will again be blank, and the *Downloaded Revision* field will have been incremented.

8. Click on *Close*.

Note that the system will automatically be restarted so that the configuration changes will take effect.

COPYING CONFIGURATION UPDATES

To copy a system's updated configuration files to a defined destination:

1. From the Systems Menu, click on *Copy Updates*.

2. If you are copying to diskette, insert a diskette into the diskette drive.

3. From the resulting dialog box, select a destination folder in one of two ways:
   a. Enter the path in the editable text field.

b. Use the dialog box tools to select the path. To use the dialog box tools:
   - Click on the drive selection arrow, then select the drive from the displayed list.
   - Use the drive's directory box to select the destination folder.
   - The editable text field will reflect the new configuration folder path.

4. Select a configuration file format. The file format pertains to the type of system you are copying the updated configuration files for. The systems are either PC-based platforms (i.e., a CSX7000) or embedded platforms (i.e., a CSX1200).

5. Select the type of revision. Choices are:
   a. *Downloaded Revision*
      This choice will be available if you have already downloaded a configuration update directly to the system. If you select *Downloaded Revision*, the downloaded configuration update files will be copied to the destination folder.
   b. New Revision
      This choice will be available if you have generated updates, but have not downloaded them yet. If you select *New Revision*, the generated configuration update files will be copied to the destination folder.

6. Click *OK*.

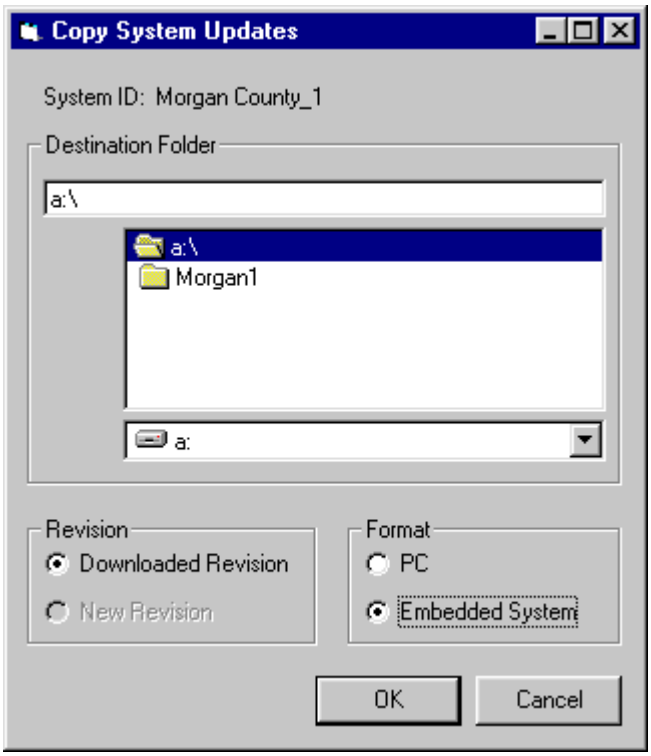
7. You should see a message reporting that the files have been successfully copied. If the message includes warnings, correct any errors described in the warnings.

8. If you will be taking the copy of the updated configuration files and copying them onto the system (for example, taking a diskette to a remote site and copying the files onto the system) you will want the database to reflect that the updates have been downloaded. Click *Mark Updates as Downloaded*. The *Updates Generated* field will again be blank, and the *Downloaded Revision* field will have been incremented.

9. Click on *Close*.

The following sample dialog box would result from copying the updated configuration files for site Morgan County, system Morgan County_1 to a diskette in drive a, folder *Morgan1*. The revision

that is being downloaded is the downloaded revision. As indicated by the format selection, System Morgan County_1 is an embedded platform.



SFVRA DATABASE DATA

Generating, downloading, and resetting SFVRA database data is done from the SFVRA-CFG's Export Configuration Menu. To get to that menu:

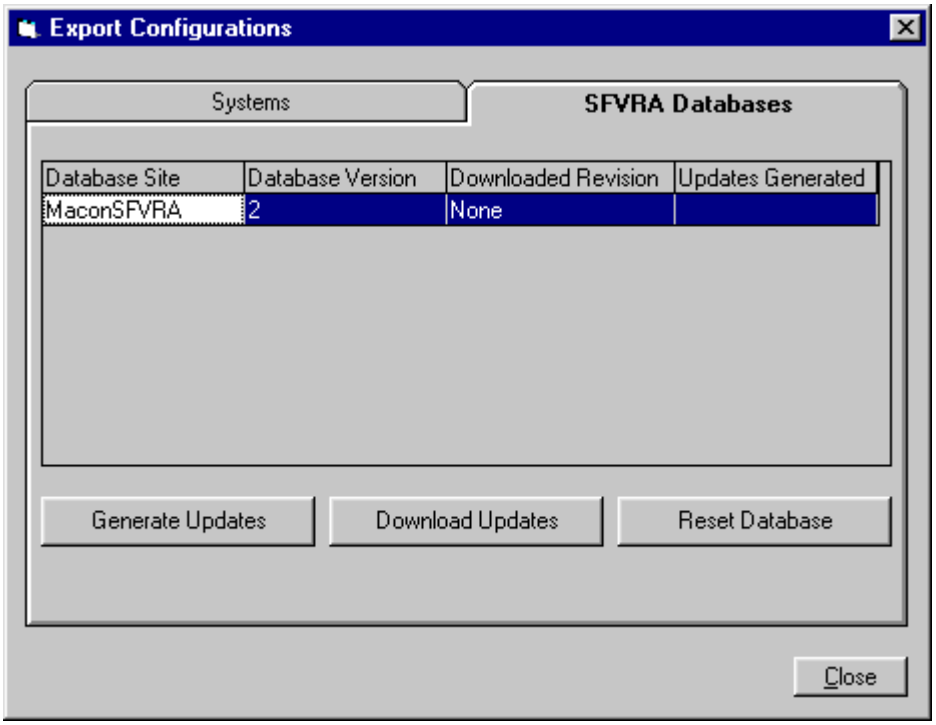
From the menu bar, click on *Options*, then click on *Export Configurations*, or simply click on the toolbar. Click on the *SVFRA Databases* tab to bring the SFVRA menu to the forefront.

Instructions for generating, downloading, and resetting SFVRA database data are described in the following sections.

GENERATING SFVRA DATABASE DATA

To generate a system's SFVRA database data:

1. Click on the Database Site of choice. In the screen shown below, *MaconSFVRA* has been selected.



2. Click on *Generate Updates*.

3. You should see a message stating that the update for the system has generated successfully. If the message includes warnings, correct any errors described in the warnings.

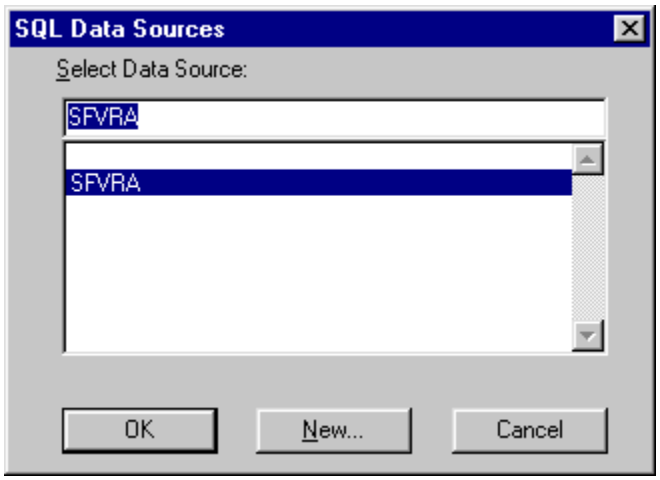
4. Click *Close*. Note that the Updates Generated field displays *YES* (it was previously blank). This indicates that the updated configuration files are ready for downloading.

DOWNLOADING SFVRA DATABASE DATA

To download a system's SFVRA database data:

1. From the SFVRA Menu, click on *Download Updates*.

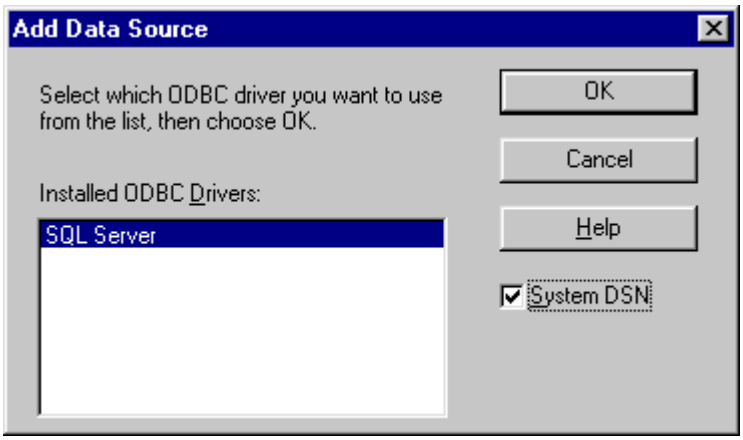
2. Select a data source for your device from the displayed list. The screen for the data source may vary depending on the version of ODBC driver you are using. We provide an example screen below.



Note that your SFVRA data source will not appear on the list unless you have configured an ODBC data source name for the source. This can be done through your device's Control Panel (use the instructions provided in *ODBC Setup*, substituting SFVRA information where needed). You can also configure a data source through the above menu.

The following directions apply to the above menu. Your screen, as noted above, may appear differently, but should generally ask for the same information.

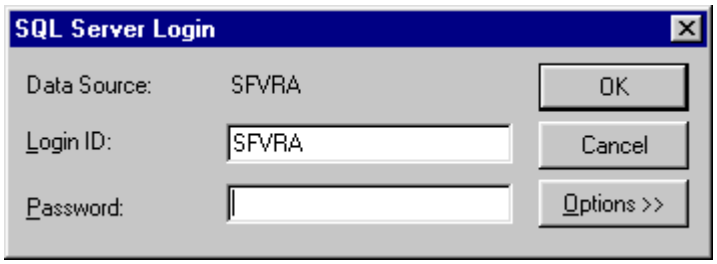
a. Click on *New*. The following screen will be displayed.



b. Select SQL Server as the Installed ODBC Driver.
c. Click on *OK*.
d. Click on System DSN (so that a check mark appears next to it).
e. Click on *OK*.
f. Enter the data source name.
g. For *Server*, select the device on which the SQL server was installed.

h. Click on *Options*. Deselect *Generate Stored Procedure for Prepared Statement*. Click *OK*.
i. Click on *Close*.

3. From the SQL Server-Login (shown below), click OK.



4. You should see a message reporting that your SFVRA download was successful. If the message includes warnings, correct any errors described in the warnings.

5. Click on *Close*.

6. The Updates Generated field will again be blank, and the Downloaded Revision field will have been incremented.

7. Click on *Close*.

RESETTING SFVRA DATABASE DATA

If you reset the SFVRA database data, the *Downloaded Revision* field will change to *None*, and a flag is set that will trigger a complete download of the data as opposed to an incremental download; it will clean out the SFVRA database before it downloads the new data.

There are two situations that call for an SFVRA database reset:

1. If an error occurs in the download process, and the data in the SFVRA database is therefore corrupted, you will want to reset the SFVRA database, generate a new update, and download the updated SFVRA data.

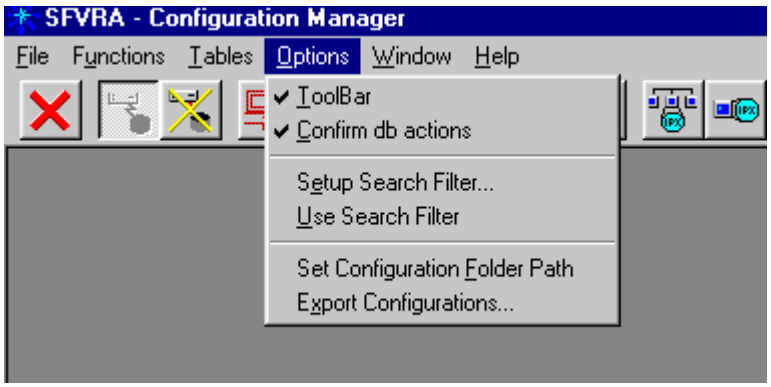
2. If local changes have been made that conflict with changes made centrally, you may want to reset the SFVRA database, generate a new update, and download the updated SFVRA data.

To reset the SFVRA database data, click on *Reset Database* (on the SFVRA Databases screen).

USING SFVRA-CFG OPTIONS

OVERVIEW

The information in this chapter provide instructions for using the SFVRA-CFG options available through the menu bar (as shown below).

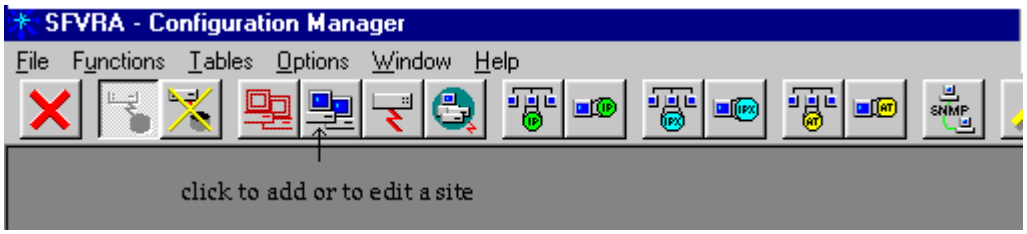


Available options include:

- setting tool bar display
- confirming database actions
- setting up and using search filters
- setting the SFVRA-CFG configuration folder path
- exporting configurations (we describe this option in detail in a separate chapter, *Exporting Configuration Files*)

SETTING THE TOOL BAR DISPLAY

If you have a mouse, the icons on the tool bar provide a shortcut to configuration functions such as creating site templates, configuring site information, and configuring connection groups. For example, you can quickly add a new site or edit existing sites by clicking on the site icon.



If you forget which task an icon performs, simply move cursor so that it's touching the icon, and text will appear below the icon, describing the icon's function.

To turn off the ToolBar display:

1. Selection *Options* from the menu bar.

2. A check mark next to *ToolBar* indicates that the display option is activated. Click on *ToolBar* to remove the check mark.

3. The display option is now deactivated.

CONFIRMING DATABASE ACTIONS

When you make a change to the SFVRA-CFG database (for example, when you add a site) you will be asked if you are sure you want to make that change. You can make a configuration change so that you are no longer asked, "*Are you sure you want to ...*"

To turn off the confirming database actions option:

1. Select *Options* from the menu bar.

2. A check mark next *Confirm db actions* indicates that the option is activated. Click on *Confirm db actions* to remove the check mark.

3. The option is now deactivated.

Note: There are certain database changes that will not allow you to proceed until you confirm the change. For example, you will not be able to configure further site information until you complete the required site information on the first dialog screen, click on *Add*, then confirm that you do want to add the site.

It is also important to note that once you answer "*Yes*" to the prompt asking if you are sure you want to make the change, that change will remain in the database, even if you click on *Cancel*.

Because of this, you may want to leave the confirming database actions option activated. The confirming messages will help to keep you up-to-date on what you have saved to the database.

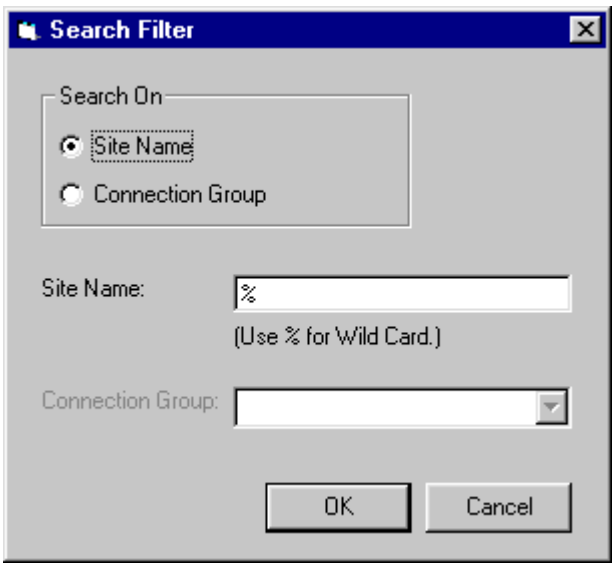
SETTING UP AND USING SEARCH FILTERS

If you have a large network, you may find the search filter option useful. Through the search filter, you can control what information is displayed. For example, if you want to make some changes to a specific site's configuration data, you could define a filter for that site name, then activate the filter. After the filter is activated, when you open windows by selecting menu options or tool bar options, information will only be displayed for the site name you specified. The filter eliminates all other site information, streamlining the information you work with. You may later deactivate the filter. You may also filter the database using a specific connection group.

To define a search filter:

1. Select *Options* from the menu bar.

2. From the resulting menu, select *Setup Search Filter*. The following screen will be displayed:

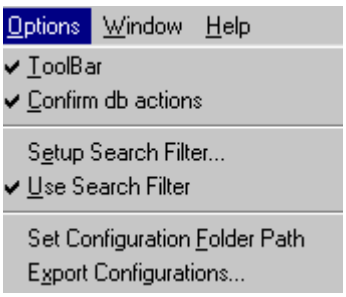


3. To setup a search filter for a site name, make sure *Site Name* is selected as shown above, then in the Site Name dialog box, enter the target site name. Click *OK*.

4. To setup a search filter for a connection group, click on *Connection Group*, then click on the connection group selection arrow, and select the connection group from the displayed list of previously configured connection groups. Click *OK*.

To use the search filter:

1. Click on *Use Search Filter* (As shown below, this appears on the menu after *Setup Search Filter*). This will activate the filter. A check will appear next to the *Use Search Filter* option once it has been activated.



2. Once *Use Search Filter* has been activated, information will only be displayed as designated by the search filter. For example, if you setup a search filter for site *Manchester* and then activate

that filter, then you select *Sites* from the Functions Menu, only information for site *Manchester* will be displayed.

To deactivate the search filter:

1. Click on *Use Search Filter* again. The check will no longer appear.

2. Once *Use Search Filter* has been deactivated, you will again see information for all sites and for all connection groups when windows are reopened or refreshed.

SETTING THE SFVRA-CFG CONFIGURATION FOLDER PATH

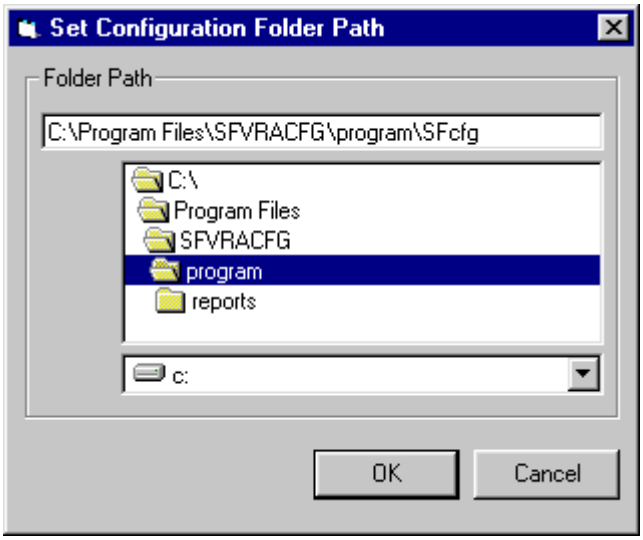
The default path for the SFVRA-CFG configuration folder is:

```
C:\Program Files\SFVRACFG\Program\Sfcfg
```

To change the configuration folder's path:

1. Select *Options* from the menu bar.

2. Click on *Set Configuration Folder Path*. You will see the following screen:



3. Change the folder path in one of two ways:
   a. Highlight the existing folder path then type in the new path.
   b. Use the dialog box tools to create the new path. To use the dialog box tools:
      - Click on the drive selection arrow, then select the drive from the displayed list.
      - Use the drive's directory box to select the destination folder.
      - The screen will reflect the new configuration folder path.

ROUTINE MAINTENANCE

OVERVIEW

This chapter provides instructions for performing routine SFVRA-CFG maintenance such as:

- performing a configuration back up
- upgrading SFVRA-CFG application software
- upgrading SFVRA-CFG database software

CONFIGURATION BACK UP

The SFVRA-CFG's database data and the SFVRA-CFG application's configuration data is critical to the SFVRA-CFG's operation. We strongly suggest that you back up this data in case you ever need to restore it.

The SFVRA-CFG's database data is stored using either an MS SQL Server or MS Access. Use the available MS SQL Server or MS Access tools to perform backups of the SFVRA-CFG database.

As a default, the SFVRA-CFG's application configuration data is stored on the same hard drive where the application is installed. The default path is as follows:

`C:\Program Files\Sfvracfg\Program\Sfcfg`.

Use available Windows 95/NT tools to back up this folder. For example, use the Windows 95/NT Explorer to make a copy the `Sfcfg` folder, then store the copy of the folder for backup purposes.

UPGRADING SFVRA-CFG APPLICATION SOFTWARE

SFVRA-CFG software must be upgraded on the system containing the SFVRA-CFG Database as well as on any system that runs the SFVRA-CFG application. During the software upgrade, you will be given the option of upgrading:

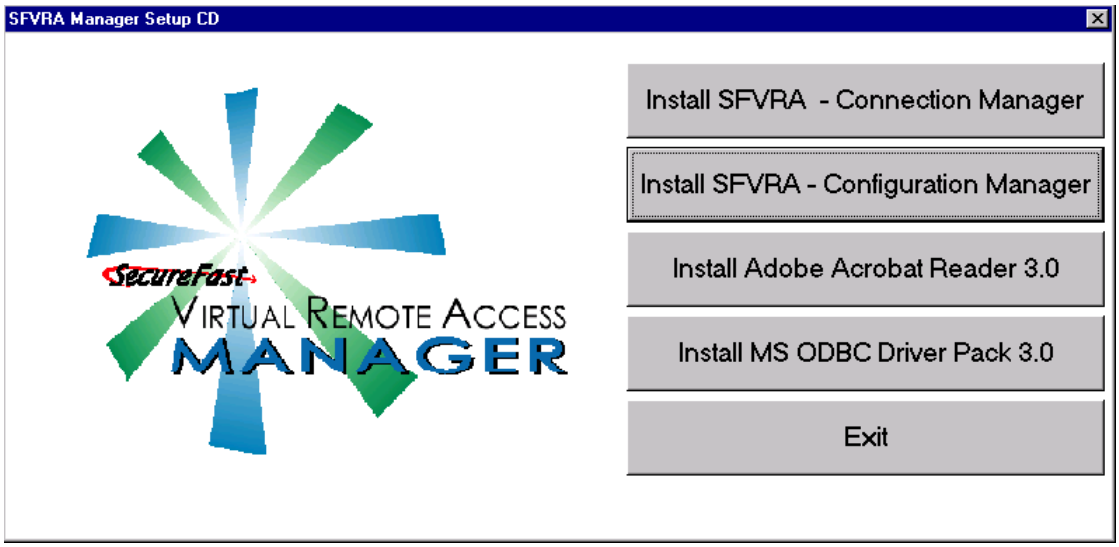
- Program and Help Files
- SFVRA-CFG Database Setup Utility
- Documentation

If you are using MS SQL Server as your database, you may upgrade all components on one system if you are running the SFVRA-CFG application on the same system containing the MS SQL Server.

Upgrade SFVRA-CFG software using the following steps:

1. Close any active applications.

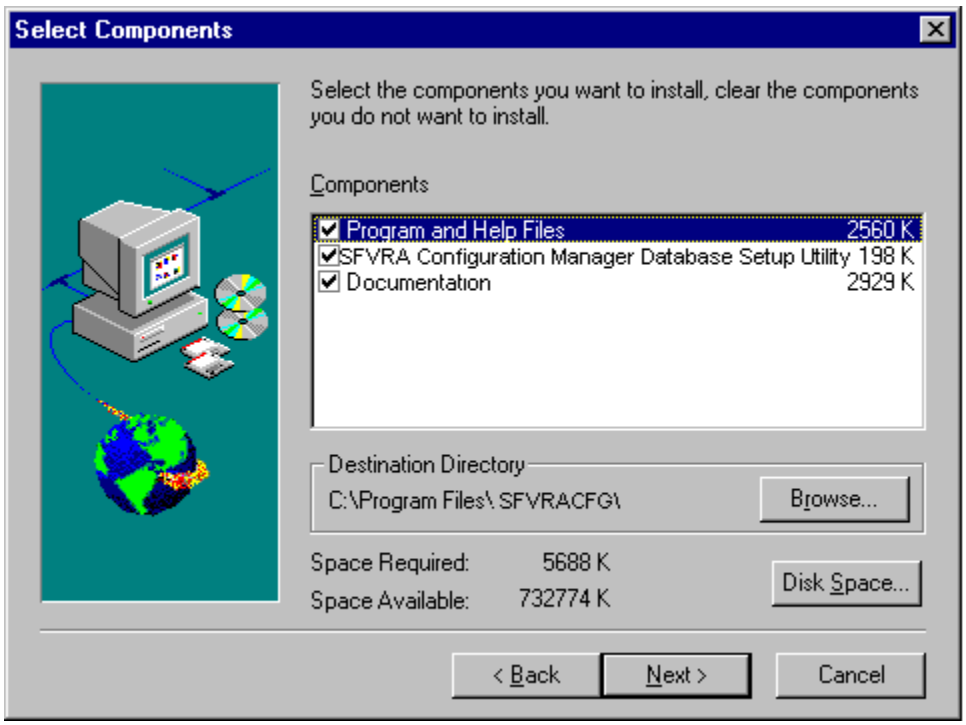
2. Insert the SFVRA-CFG CD into the CD-ROM drive. If, as is usually the case, your CD-ROM is setup for AutoPlay, the following screen will automatically be loaded:



To manually load the above screen, select *Run* from the Start Menu. Enter *<CD-ROM drive>:\SCFGCD.EXE* as the program to open, then select *OK*.

3. Click on *Install SFVRA Configuration Manager*.

4. The following screen will be displayed, allowing you to select which SFVRA-CFG components you want to upgrade. Make sure a check appears next to the components you wish to upgrade.


Select Components
Select the components you want to install, clear the components you do not want to install.
Components
Program and Help Files 2560 K
SFVRA Configuration Manager Database Setup Utility 198 K
Documentation 2929 K
Destination Directory
C:\Program Files\SFVRACFG\
Browse...
Space Required: 5688 K
Space Available: 732774 K
Disk Space...
< Back
Next >
Cancel

5. Follow onscreen instructions to complete the upgrade.

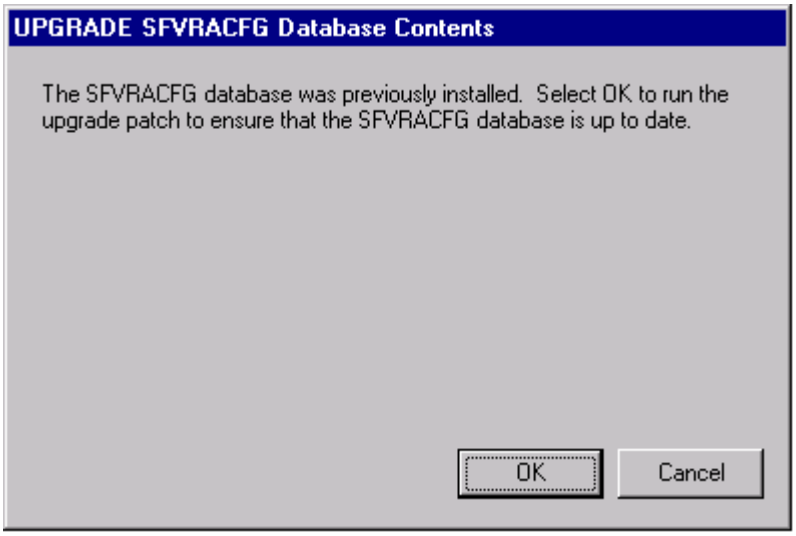
UPGRADING SFVRA-CFG DATABASE SOFTWARE (ONLY IF USING MS SQL SERVER)

1. Close active applications.

2. Upgrade the SFVRACFG database.
   a. The SFVRACFG database is created by the SFVRA-CFG Database Setup Utility. You may choose to run this utility when upgrading SFVRA-CFG software. If you choose not to run the utility while upgrading the software you may start the utility after completing the software upgrade. To do this, from the Start menu \ Programs \ SFVRA Configuration Manager, select *SFVRA-CFG Database Setup*.
   b. Enter the *sa* password, if necessary, and click *OK*. The SQL Setup program executes.

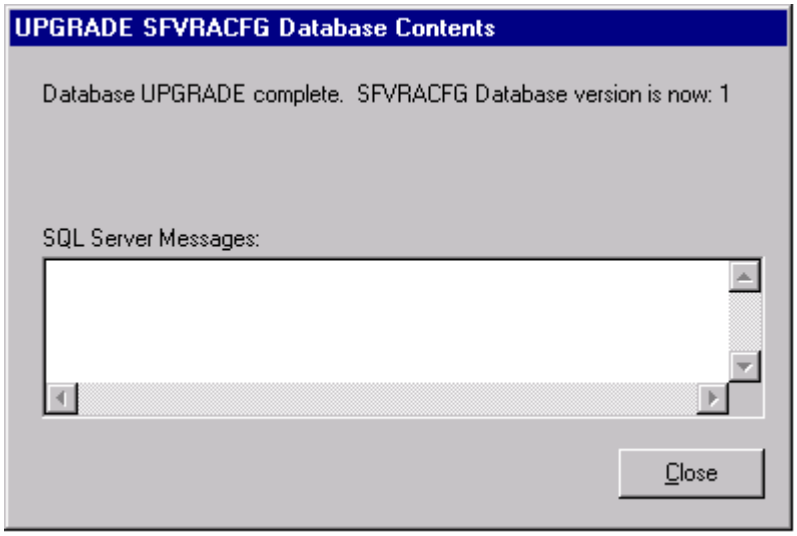
3. Follow the onscreen instructions to complete the installation.

4. If the SQL Server is installed on this machine, the SQL Setup program will be executed to update the database tables. The following screen appears:


UPGRADE SFVRACFG Database Contents
The SFVRACFG database was previously installed. Select OK to run the upgrade patch to ensure that the SFVRACFG database is up to date.
OK
Cancel

5. Click *OK* to upgrade the database.

6. When the upgrade procedure is complete, the following screen appears:


UPGRADE SFVRACFG Database Contents
Database UPGRADE complete. SFVRACFG Database version is now: 1
SQL Server Messages:
Close

Ensure that no errors occurred. Scroll through the list of SQL Server Messages, if any.

7. Click *Close*.

SYSTEM WORKSHEETS

The worksheets included in this appendix will be helpful in configuring and managing your system. They capture important network information. To see examples of completed worksheets, refer to the *Example Networks Guide.*

Worksheets included in this appendix are:

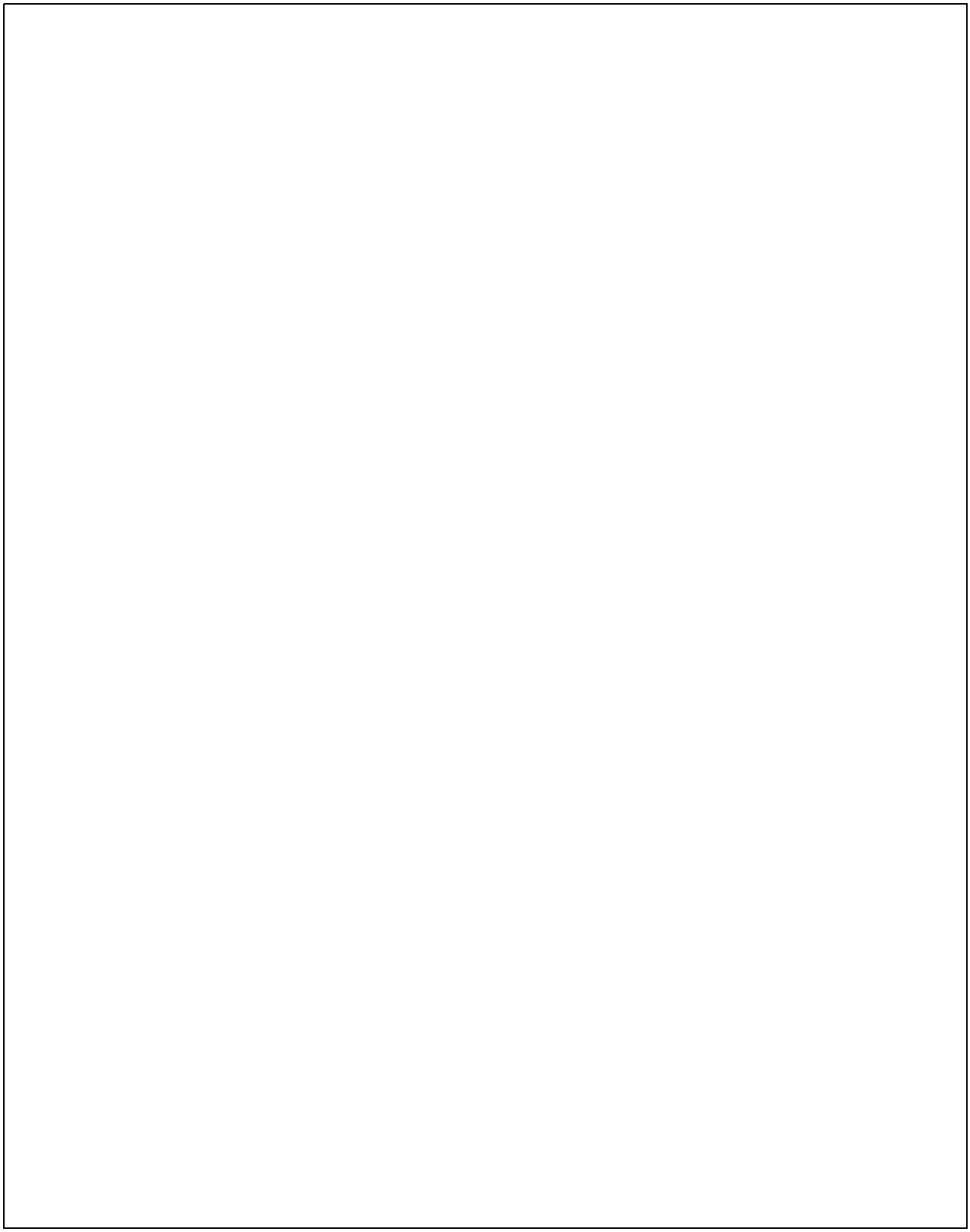
1. Network Topology Worksheet. This worksheet identifies the following information:
   - The Users or Remote Sites in your network.
   - The telephone numbers associated with the Users or Remote Sites in your network.
   - IP/IPX/AppleTalk information related to the Users or Remote Sites in your network.
   - Bridge addresses related to the Users or Remote Sites in your network.
   - Password information related to the Users or Remote Sites in your network.

2. System Details Worksheet. This worksheet identifies the following information for each SFVRA-CFG in your network:
   - The resource details for each adapter in your SFVRA-CFG. Note the switch type.
   - Details on each ISDN line attached to your SFVRA-CFG. If a line has more than one SPID, use an extra worksheet line to record that SPID and its associated directory number.
   - Details on any configured accesses.

3. The Device Information Worksheet identifies device information for one device. Complete a worksheet for each of your network's remote devices.

4. Use the Bridging and Routing Information Worksheets to summarize your particular setup (from the Network Topology Worksheet) to ease the configuration process.

NETWORK TOPOLOGY



SYSTEM DETAILS

System Name: _____ PAP Password:_____ CHAP Secret:_____

RESOURCES

Type	Slot	Switch type	Synchronization type

LINES

BRI Lines

Name	Slot	Port	Line type	Call screen	TEI	SPID	Directory number

PRI Lines

Name	Slot	Port	Framing type	Line coding	Sig. method	Line build-out

V.35 and RS232 Lines

Name	Slot	Port	Device/Network	Idle character

ACCESSES

Dedicated Accesses

Over ISDN:

Line name	Data rate	Bearer channels	Line protocol	Device tied to this access
	❒ 56 Kbps ❒ 64 Kbps			
	❒ 56 Kbps ❒ 64 Kbps			
	❒ 56 Kbps ❒ 64 Kbps			
	❒ 56 Kbps ❒ 64 Kbps			

Over Serial connection:

Line name	Clocking	Data rate	Line protocol	Device tied to this access
	❒ Internal ❒ External			
	❒ Internal ❒ External			
	❒ Internal ❒ External			
	❒ Internal ❒ External			

X.25 Accesses

Over ISDN:

Line name	Access name	X.121 address of local DTE	Data rate	Bearer channels	Virtual circuits (PVCs)

Over serial connection:

Line name	Access name	X.121 address of local DTE	Clocking	Data rate	Virtual circuits (PVCs)
			❒ Internal ❒External		

Frame Relay Accesses

Over ISDN:

Line name	Access name	Data rate	Bearer channels	DLCI	PVC name	CIR	EIR
		❒ 56 Kbps ❒ 64 Kbps					

Over serial connection:

Line name	Access name	Clocking	Data rate	DLCI	PVC name	CIR	EIR
		❒ Internal ❒ External					

DEVICE INFORMATION

Device Name: _____

Calling (ISDN, FR, etc.) Information

Line Protocol	
Base Data Rate	
Initial Data Rate	
Max Data Rate	
Dial-Out Number(s)	

X.25 Information

PVC	
SVC	

Authentication Information:

PAP Password	
CHAP Secret	
IP Host ID	
Bridge Ethernet Address*	
Bridge Password*	
CLID(s)	

* HDLC Bridge only

Frame Relay Information

DLCI	

Protocol for this particular device?

Bridge

Bridging enabled?	❒ enabled ❒ disabled
Make calls for bridged data?	❒ enabled ❒ disabled
For IP RLAN, IP (Sub-) network number	
For IPX RLAN, external network number	

IP

IP enabled?	❒ enabled ❒ disabled
IP Address (on WAN link)	❒ 0.0.0.0 if unnumbered link
Make calls for IP data?	❒ enabled ❒ disabled
IP input filter?	
IP output filter?	

IPX

IPX enabled?	❒ enabled ❒ disabled
Callable by IPX?	❒ enabled ❒ disabled
IPXWAN protocol?	❒ enabled ❒ disabled
IPX routing protocol?	❒ none ❒ RIP/SAP ❒ triggered RIP/SAP
IPX spoofing?	

AppleTalk

AppleTalk enabled?	❒ enabled ❒ disabled
AppleTalk Address	
Make calls for AT data?	❒ enabled ❒ disabled
AT Routing Protocol	

BRIDGING AND ROUTING INFORMATION

BRIDGING

Bridging	❒ enabled ❒ disabled	
Mode of Operation	❒ restricted ❒ unrestricted	
Bridge Filters		
Bridge Dial Out/ Known Connect List		

IP ROUTING

IP Routing	❒ enabled ❒ disabled	
Mode of Operation	❒ router ❒ IP host	

Network Interface Information

LAN	Name			
	IP address			
	Mask			
Unnumbered WAN	❒ need ❒ don't need			
	Input filters			
	Output filters			
Remote LAN	Name			
	IP address			
	Mask			
	Input filters			
	Output filters			
Traditional WAN	Name			
	IP address			
	Mask			
	Input filters			
	Output filters			
Direct Host WAN	Name			
	IP address			
	Mask			
	Input filters			
	Output filters			
IP Host Mode	IP address			
	Mask			
	Input filters			
	Output filters			

IP ROUTING, CONTINUED

Static Routes

Destination network number	Mask	Next hop
❒ default?		
❒ default?		
❒ default?		
❒ default?		

IPX ROUTING

Routing Information

IPX routing	❒ enabled ❒ disabled
Internal network number	

Network Interface Information

LAN	Name			
	External network number			
Remote LAN	Name			
	External network number			

Static Routes

Destination network number	Next hop
❒ Int. ❒ Ext.	
❒ Int. ❒ Ext.	
❒ Int. ❒ Ext.	
❒ Int. ❒ Ext.	
❒ Int. ❒ Ext.	
❒ Int. ❒ Ext.	

NetWare Static Services

Service name	Type	Internal network number	Node number	Socket number

APPLETALK ROUTING

AppleTalk Routing/Port Information

AppleTalk routing	❒ enabled	❒ disabled		
LAN	Name			
	Port number			
	Network type	❒ extended ❒ nonextended		
	Netwk range/ number			
	AppleTalk address			
	Zone name(s)			
WAN	Name			
	Network type	❒ extended ❒ nonextended	❒ extended ❒ nonextended	❒ extended ❒ nonextended
	Netwk range/ number			
	AppleTalk address			
	Zone name(s)			
Unnumbered WAN	❒ need ❒ don't need			
MAC Dial In WAN	Network type	❒ extended ❒ nonextended	❒ extended ❒ nonextended	❒ extended ❒ nonextended
	Netwk range/ number			
	AppleTalk address			
	Zone name(s)			
WAN (Remote LAN)	Name			
	Network type	❒ extended ❒ nonextended	❒ extended ❒ nonextended	❒ extended ❒ nonextended
	Netwk range/ number			
	AppleTalk address			
	Zone name(s)			

AppleTalk Port Static Routes

Network type to be accessed	Destination network range	Next hop address	Next hop name	Number hops	Zone name(s)
❒ extended ❒ nonextended					
❒ extended ❒ nonextended					

GETTING ASSISTANCE

REPORTING PROBLEMS

For a fast response, please take the time to fill out the System Problem Report to inform us of any difficulties you have with our products. A copy of this report can be found at the end of this chapter. This report provides us with important information to diagnose and respond to your questions. Please pay special attention to the following areas:

FAX Header
The System Problem Report has been designed as a FAX form. Please fill in all information in this area before you FAX the report to Cabletron Systems. If you plan to mail the System Problem Report, please fill in the company information in this section for reference information.

Software
Please fill in the following sections:
- Release, Issue, and Version (From the VERsion command.)

Hardware
Select the Platform and resources that you are using.

Problem
Please fill in the following sections:
- Type (Software, Hardware, Unknown.)
- Occurrence (Reproducible, Intermittent, Single Occurrence.)
- Original Number (This field is for your use. Enter your problem tracking number, if desired, for future reference.)
- Description (Briefly describe the problem you are experiencing.)

Description (including sequence of events):
Briefly describe the problem you are experiencing. As best you can, describe the events or conditions that led to the problem you are experiencing.

Please send the System Problem Report form and any extra information (for example, line traces, system reports, and configuration files) that you have.

CONTACTING CABLETRON SYSTEMS

You can call us directly at:

Phone: (603) 332-9400
FAX: (603) 337-3075 fax

or, you can send email to us at:

support@ctron.com

DATE: _____ NUMBER OF PAGES INCLUDING THIS PAGE: _____

TO: CUSTOMER SERVICE
Cabletron Systems
(603) 332-9400 PHONE
(603) 337-3075 FAX

FROM: _____
COMPANY:_____
ADDRESS: _____
_____
PHONE: _____
FAX: _____

CABLETRON SYSTEMS
SYSTEM PROBLEM REPORT

SOFTWARE

Release: _____ Issue: _____ Version: _____

HARDWARE

Platform		Resources	
__ CSX154	__ 9W006-200	__ Ethernet-1	__ BRI-4
__ CSX155	__ 9W006-400	__ Ethernet-2	__ V.35
__ CSX1000	__ 9W006-220	__ PRI-8	__ RS232
__ CSX1200	__ 9W007-200	__ PRI- 23	__ DM8
__ CSX5500	__ 9W007-400	__ PRI- 23/30	__ DM24
__ CSX6000	__ 9W007-220	__ Expander	__ DM24+
__ CSX7000		__ BRI-1	__ DM30

PROBLEM

Type	Occurrence
__ Hardware	__ Reproducible
__ Software	__ Intermittent
__ Unknown	__ Single Occurrence

DESCRIPTION (including sequence of events prior to problem occurrence):

_____

_____

_____

_____

_____

_____

CABLETRON SYSTEMS USE ONLY

Control No:	Priority:	Date Received:
Resolution:		

INDEX

A

access information 64
accesses 83
ACFC values 56
admin 30
admin access level 145
administrative session configuration 60
A-law 47
AMI coding 45
AppleTalk 129
  network types 130
  ports 133, 139
  protocols 129
  segment information 129
  static routes 134, 140
  system information 137
  zones 131
AppleTalk information 53, 69
authentication
  information 61
  protocols 16
  traps 54

B

B8ZS coding 45
backing up data 160
bandwidth
  limitations 63
bandwidth reservation 76
base data rate 62
BCP 16
bearer channels 84
BRI resources 43
bridge MAC address security
  Ethernet address 75
bridging
  bridge age time 48
  bridging mode 48
  protocol configuration 70
  Spanning Tree protocol 48
  unrestricted mode 48
bridging information 48

C

call control information 57
call interval 57
call screening 83
CCP 16
circuits
  call screening 83
  configuring 79
  data links 81
  definition 15
  properties 80
CLIDs
  adding 94
clocking 44
communities (SNMP) 144
compression 64
compression control protocol 16
configuration files 148
  copying updates 150
  downloading updates 150
configuration updates
  generating 149
configuring circuits 79
connection group
  filtering 158
connection groups
  adding 85
connection information
  modifying 92
connections information 61
  access information 64
  authentication 61
  protocols 65
  restrictions 62
contact information 73
conventions (guide conventions) 10
copying configuration files 150

D

D4 framing type 45
data
  backing up 160
data line idle character 46
data links 81
data rate
  base 62
  initial 62
  maximum 63
data source
  SQL 154
database
  searches 157
  SFVRA 152
database installation 22
dedicated accesses 84
default line protocol 59

default profile 76, 97
default profiles 77
default routes 30
default static route 103
device authentication name 71
device requirements 18
devices
  remote ISDN 17
digital modem resources 47
directory number 80, 82
doubleframe framing type 45
downloading
  configuration files 150
  SFVRA database data 153
duplicate menu option 33
duplicating site templates 42
dynamic address assignment 66

E
echo-request frames 56
Emergency Telnet server 60
encapsulation type 49, 108
entry aging time 124
entry aging time (IPX RIP and SAP) 52
ESF framing type 45
Ethernet encapsulation type 108
Ethernet II encapsulation 52
exporting configuration updates 148
extended network type 130
external network number 121

F
filtering 157
filters
  configuring IP filters 118
flags (data line idle character) 46
frame timeout action 59

G
generating
  configuration updates 149
  SFVRA database data 153
generating routes
  for connected LANs 117
global PPP options 55
guest access level 145

H
help
  getting assistance 172
host routes propagation 50
hunt group number 80

I
initial data rate 62
installation
  MS SQL Server 19
  ODBC 19
  SFVRA-CFG database 22
  SFVRA-CFG software 21
interface types
  definitions 105
internal network number 126
interoperability
  devices 16
  overview 16
  protocols 16
IP address negotiation initiation 56
IP filters 118
IP information 49, 65
IP network
  general concepts 99
  subnet information 102
  systems information 112
IP pool address 106
IP protocol
  defined 99
ipconfig 30
IPCP 16
  configuration 56
IPX
  expert options 123
  external network number 121
  information 51, 66
    spoofing 67
  interface types 122
  internal network number 126
  IPX WAN 66
IPX network
  segment information 120
  systems information 125
IPXCP 16
ISDN
  network devices 17
ISDN B-channel usage traps 54
ISDN throughput monitor 58
isdnUsageHigh trap 54
isdnUsageNormal trap 54

L
LAN interface 105
LAN port priority 49
layer 2 protocol 64

LCP 16
  configuration 56
line build out 45
line coding 45
line interface type 44
line type 46
link failure detection 56
login accounts 25
login id 30

M
macdialin 134, 140
maintenance 160
manage logins 25
managed sites (SNMP) 146
management groups (SNMP) 143
marks (data line idle character) 46
master clocking 45
max configure 55
max failure 55
max table entries 52
max terminate 55
maximum data rate 63
menu options
  descriptions 33
menu selections 33
mesh network 89
message packet handling 68
metric value
  definition 111
MIB level access 145
minimum fragment size (multilink) 57
MLP 16
modifying connection information 92
modifying star configurations 87
MS SQL Server
  installation 19
MTU 108, 123
MTU value 49, 52, 108
mu-law 47
multiframe framing type 45

N
NET5 44
network control protocols
  BCP 16
  IPCP 16
network interfaces
  examples 99
  overview 99
network number 134
network topology worksheet 165
next hop
  for IP subnets 111, 136
next hop site name 136
node ID 134
nonextended network type 130

O
ODBC
  installation 19
options
  for site templates 47
overview
  system 11

P
packet encapsulation type 49, 51, 108, 123
packet handling (spoofing) 68
password 30
path cost 49
PCF values 56
PCM 47
physical resources 43
  BRI 43
  digital modem 47
  PRI 44
  V.35 and RS232 46
ports (AppleTalk) 133
PPP
  information 55
  multilink options 56
  STAC-LZS sequence number 64
PRI resources 44
primary rate ISDN lines
  synchronization type 44
problems
  getting assistance 172
product code 36, 73
profile
  default 77
profiles
  default 76, 97
properties
  circuits 80
protocol view
  definition 15
protocols 16
  AppleTalk 69, 129
  bridging 70
  information 65
  IP 65
  IPX 66
pswd 30

R
receive control 50, 52
refresh menu option 33
reports 147
resetting the SFVRA database 155
respond control 50, 52
restart timer (PPP) 55
restricted bridge mode 48
restriction information 62
RIP
  configuration 50
  IP host routes propagation 50
RIP information (IP) 108
RIP propagation control 111
RIP services 39
RIP/SAP configuration 123

S
sample rate (throughput monitor) 58
SAP configuration (IPX) 52
searches 157
security
  site 71
security information 60
segment information
  IPX network 120
semi-permanent connections 64
send control 50, 52
send frequency 52
serialization packet handling 68
session inactivity timeout 60
SFVRA database 152
  downloading 153
  generating 153
  resetting 155
SFVRA database table 38
SFVRA services 39
SFVRA-CFG
  application
    device info 11
  database
    device info 11
  device requirements 18
  installation 19
  model 12
  network overview 12
  system components 17
  upgrading application 160
  upgrading database 162
signaling method 45
simulated switch type 43, 44
site
  adding 71
  definition 13
  filtering using site names 158
  security 71
site contact information 73
site template
  adding 41
  AppleTalk information 53
  bridging information 48
  call control information 57
  configuring options 47
  connections information 61
  default line protocol 59
  duplicating 42
  IP information 49
  IPX information 51
  physical resources 43
  PPP information 55
  security information 60
  SNMP information 54
slave clocking 44
SNAP encapsulation 51
SNAP encapsulation type 108
SNMP
  communities 144
  managed sites 146
  management groups 143
  MIB level access 145
  site template information 54
  trap receivers 145
software
  installation 21
  release version 75
  upgrading 162
Spanning Tree protocol 48
SPID information 82
spoofing 67
  packet handling 68
SQL data source 154
STAC-LZS sequence number 64
star configurations
  modifying 87
static routes
  AppleTalk 134
  for IP subnets 109
  overview 101
subaddress
  call screening 83
subnet address
  definition 104

subnet information
IP network 102
subnet mask
definition 104
switch country 43, 44
synchronization type 44
system
client requirements 18
components 17
maintenance 160
overview 11
server requirements 18
system details worksheet 166
system ID 73

T
TCP port number 60
TEI negotiation 44, 45
Teleos Simulator 43, 44
telephone numbers
adjusting 92
for call screening 83
Telnet sessions 60
throughput monitor 58
tool bar 156
transmit broadcast address
definition 106
trap receivers (SNMP) 145
trigger number 58
triggered RIP / SAP 66
type 20 packet forwarding 67

U
unrestricted bridge mode 48
upgrading
application software 160
database software 162
user access level 145
user database
selecting 71
using this guide 8
utilization percentage (throughput monitor) 58

V
V.35 resource 46
v2 authorization password (IP RIP) 51

W
WAN (Mac Dial In) 134, 140
WAN (remote LAN) interface 106
WAN interface 106
WAN peer type 66
watchdog spoofing 67
window size 58
worksheets 164

Z
zones (AppleTalk) 131